Attorney Docket No. 1046.1308

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Mikako OCHIAI

Application No.: To be Assigned | Group Art Unit: To be Assigned

Filed: January 30, 2004 | Examiner: To be Assigned

For: ABNORMALITY DETECTION METHOD, ABNORMALITY DETECTION PROGRAM, SERVER, COMPUTER

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-049255

Filed: February 26, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: May 30, 2004

By: _____

Gene M. Garner II
Registration No. 34,172

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

opi1711

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ２月２６日

出 願 番 号
Application Number: 特願２００３－０４９２５５

[ST. 10/C]: ［ＪＰ２００３－０４９２５５］

出 願 人
Applicant(s): 富士通株式会社

２００３年１０月２７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０８８６５１

【書類名】　特許願
【整理番号】　0253352
【提出日】　平成15年 2月26日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/00
G06F 13/00
【発明の名称】　異常検出方法、異常検出プログラム、サーバ、コンピュータ
【請求項の数】　5
【発明者】
【住所又は居所】　東京都稲城市大字大丸１４０５番地　株式会社富士通パソコンシステムズ内
【氏名】　落合　美香子
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100089244
【弁理士】
【氏名又は名称】　遠山　勉
【選任した代理人】
【識別番号】　100090516
【弁理士】
【氏名又は名称】　松倉　秀実
【連絡先】　０３－３６６９－６５７１
【手数料の表示】
【予納台帳番号】　012092
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705606

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　異常検出方法、異常検出プログラム、サーバ、コンピュータ

【特許請求の範囲】

【請求項１】

電子メールの送信を依頼するコンピュータと該コンピュータからの依頼に応じて電子メールを送信するサーバとからなる電子メールシステムで実行される前記コンピュータの動作異常を検出する方法であり、

前記コンピュータによる電子メールの送信依頼履歴に係る依頼履歴情報を参照するステップと、

前記サーバによる電子メールの送信履歴情報を参照するステップと、

前記依頼履歴情報と前記送信履歴情報とを比較するステップと、

前記比較結果に基づいて前記コンピュータの動作異常を検出するステップと、からなる異常検出方法。

【請求項２】

電子メールの送信を依頼するコンピュータにネットワークを介して電子メール送信サービスを提供するサーバが前記コンピュータの動作異常を検出するためのプログラムであり、

前記サーバに、

前記コンピュータからの電子メールの送信依頼に基づき送信された電子メールに係る送信履歴情報を参照するステップと、

前記コンピュータによる電子メールの送信依頼履歴に係る依頼履歴情報を参照するステップと、

前記送信履歴情報と前記依頼履歴情報とを比較するステップと、

前記比較結果に基づいて前記コンピュータの動作異常を検出するステップと、を実行させる異常検出プログラム。

【請求項３】

電子メール送信サービスを提供するサーバにネットワークを介して電子メールの送信を依頼するコンピュータが、当該コンピュータの動作異常を検出するためのプログラムであり、

コンピュータに、

前記サーバに電子メールの送信を依頼した電子メールに係る依頼履歴情報を参照するステップと、

前記サーバに蓄積されている電子メールの送信履歴に係る送信履歴情報を参照するステップと、

前記依頼履歴情報と前記送信履歴情報とを比較するステップと、

前記比較結果に基づいて動作異常を検出するステップと、

を実行させる異常検出プログラム。

【請求項４】

電子メールの送信を依頼するコンピュータに電子メール送信サービスを提供するサーバであり、

前記コンピュータから電子メールの送信依頼を受け付ける受付手段と、

前記送信依頼を受けた電子メールを送信する送信手段と、

送信した電子メールに係る送信履歴情報を蓄積する蓄積手段と、

前記コンピュータに蓄積されている電子メールの送信依頼履歴に係る依頼履歴情報を前記コンピュータから参照する履歴参照手段と、

前記送信履歴情報と前記依頼履歴情報とを比較する比較手段と、

前記比較結果に基づいて前記コンピュータの動作異常を検出する検出手段と、

を備えるサーバ。

【請求項５】

電子メール送信サービスを提供するサーバに電子メールの送信を依頼するコンピュータであり、

前記サーバに電子メールの送信を依頼する依頼手段と、

送信を依頼した電子メールに係る依頼履歴情報を蓄積する蓄積手段と、

前記サーバに蓄積されている電子メールの送信履歴に係る送信履歴情報を前記サーバから参照するサーバ履歴参照手段と、

前記依頼履歴情報と前記送信履歴情報とを比較する比較手段と、

前記比較結果に基づいて動作異常を検出する検出手段と、

を備えるコンピュータ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、異常な電子メールの送信を検出する技術に関する。特に、メールサーバを介して電子メールの送受信を行う際にコンピュータウイルスの検出を行う技術に関する。

【０００２】

【従来の技術】

コンピュータウイルスの感染源の大半は電子メールであるといわれている。一般的なウイルス対策として、ＬＡＮのようなネットワーク全体を防御するためには、ゲートウェイ用アンチウイルスサーバが利用されている。また、端末単位のウイルス対策としては、アンチウイルスソフトをインストールすることが行われている。

【０００３】

アンチウイルスサーバやアンチウイルスソフトは、予め既知のコンピュータウイルスに関する情報（例えば、パターンファイル）を有している。

【０００４】

アンチウイルスサーバやアンチウイルスソフトでは、パターンファイルと、送信されたメールやメールに添付されたデータとを比較することによりコンピュータウイルスを検出していた。

【０００５】

【特許文献１】

特開２００２－１９６９４２号公報

【０００６】

【発明が解決しようとする課題】

ところで、コンピュータウイルスには、ユーザ端末にインストールされているメールソフトのメールアドレス帳に登録してあるメールアドレス宛にコンピュータウイルス自身と同型のウイルスをメールとして送信するウイルスがある。

【０００７】

このようなコンピュータウイルスは、メール受信者のコンピュータに感染するだけでなくメールアドレス帳にある他のユーザのコンピュータにまでに感染する可能性がある。その場合、メール受信者がメールの発信者となるため、メール受信者までが加害者になりかねない。

【０００８】

しかし、従来のアンチウイルスサーバやアンチウイルスソフトは、頻繁にパターンファイルをアップデートしなければならなかった。

【０００９】

そのため、常に最新のパターンファイルにアップデートしておかなければ、パターンファイルが対応しているコンピュータウイルスしか検出することができなかった。

【００１０】

また、従来のアンチウイルスサーバやアンチウイルスソフトは、未知のコンピュータウイルスを検出できなかった。そのため、コンピュータウイルスの被害が拡大し、それが判明した後その対策がとられることが多かった。

【００１１】

そこで、本発明は、上記事項に鑑みてなされたものであり、ウイルスやその他に起因するコンピュータの動作異常を検出する異常検出方法、異常検出プログラム、サーバ、コンピュータを提供することを課題とする。

【００１２】

また、本発明は、パターンファイルの更新を要することなく、未知のコンピュータウイルスの手がかりを発見する異常検出方法、異常検出プログラム、サーバ、コンピュータを提供することを課題とする。

【００１３】

【課題を解決するための手段】

本発明は、前記課題を解決する為に以下の手段を採用した。すなわち、本発明は、電子メールの送信を依頼するコンピュータと該コンピュータからの依頼に応じて電子メールを送信するサーバとからなる電子メールシステムで実行される前記コンピュータの動作異常を検出する方法であり、コンピュータによる電子メー

ルの送信依頼履歴に係る依頼履歴情報を参照するステップと、サーバによる電子メールの送信履歴情報を参照するステップと、依頼履歴情報と送信履歴情報とを比較するステップと、比較結果に基づいて前記コンピュータの動作異常を検出するステップとからなることを特徴とする。

【００１４】

コンピュータには、電子メールの送受信が可能なパーソナルコンピュータや携帯端末等が含まれる。

【００１５】

サーバは、インターネットへの接続サービスを行うプロバイダであると好ましいがこれに限るものではない。サーバは、依頼履歴情報を参照するため、上記コンピュータから依頼履歴情報を送信させるようにしてもよい。また、サーバがコンピュータの依頼履歴をネットワークを介して参照できるようにしてもよい。

【００１６】

加えて、本発明の異常検出方法は、コンピュータの動作異常が検出されたことをそのコンピュータに報知するステップを付加すると好ましい。報知方法には、コンピュータの表示手段等にメッセージを表示する方法、或いはコンピュータ所有者（ユーザ）に電子メールを送信する方法等が好適に行われる。その他の方法として、警戒音を鳴らすようにしてもよい。

【００１７】

これによって、コンピュータのユーザは、コンピュータの異常を迅速に把握することができるため、被害が拡大するのを防ぐことができる。

【００１８】

さらに、本発明の依頼履歴情報及び／又は送信履歴情報は、コンピュータから送信された電子メールの送信先のアドレスやユーザ名等の情報、送信経路に関する情報、電子メールの送信元のアドレスやユーザ名等の情報、電子メール本文の内容、電子メールのタイトル、添付ファイルの有無、添付ファイル名等の情報を含むと好ましい。

【００１９】

また、本発明の依頼履歴情報には、例えば、コンピュータから送信を依頼した

日時（送信日時）が含まれ、本発明の送信履歴情報には、サーバが電子メールを受け付けたときの日時及び受け付けた電子メールを送信先に送信した日時を含むようにしてもよい。このように、依頼履歴情報と送信履歴情報との比較結果からウイルスの存在の有無を検出する為、ウイルス自身がメール送信機能を有するウイルスの検出が可能になる。

【００２０】

また、本発明の異常検出方法は、上記した履歴情報の比較をユーザ端末側で行っても良いし、履歴情報の比較をサーバとユーザとは異なる別の端末で行っても良い。

【００２１】

また、本発明の異常検出方法は、ウイルスのパターンからウイルスを検出するのではなく、メールの送信履歴やメールソフトの動作履歴等の依頼履歴情報からウイルスを検出するため、最新のウイルス定義情報を更新していないコンピュータであっても、ウイルスを検出することができる。つまり、本発明によれば、未知のウイルスも検出することができ、ウイルスの蔓延を未然に防止することができる。

【００２２】

また、本発明の異常検出方法は、ウイルスによる動作状態の異常を検出することに限らず、サーバ又はコンピュータの何らかの故障による動作異常を検出することにも適用することができる。

【００２３】

さらに、本発明の異常検出方法は、コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、最新に送信依頼された電子メールを含む送信履歴情報を送信確認条件に従って確認するステップとを含んでもよい。そして、前記ステップによる確認結果が所定の基準を満たした場合に、送信履歴情報と依頼履歴情報とを比較するようにしてもよい。

【００２４】

このように、コンピュータが蓄積した依頼履歴情報とサーバが蓄積した送信履歴情報の比較ステップに、サーバ自身が蓄積した送信履歴情報と送信確認条件と

を比較するステップを付加することにより、ウイルス存在の可能性を高精度で検出することが可能となる。

【００２５】

さらに、本発明は、電子メールの送信を依頼するコンピュータにネットワークを介して電子メール送信サービスを提供するサーバがコンピュータの動作異常を検出するプログラムであってもよい。本発明のプログラムは、サーバに、コンピュータからの電子メールの送信依頼に基づき送信された電子メールに係る送信履歴情報を参照するステップと、コンピュータによる電子メールの送信依頼履歴に係る依頼履歴情報を参照するステップと、送信履歴情報と依頼履歴情報とを比較するステップと、比較結果に基づいてコンピュータの動作異常を検出するステップとを実行させることを特徴とする。

【００２６】

このプログラムは、サーバ，コンピュータ，それ以外の端末の何れかのハードディスクにインストールすることにより実行可能となる。例えば、本発明の異常検出プログラムをコンピュータ側にインストールすることにより、コンピュータに、サーバに電子メールの送信を依頼した電子メールに係る依頼履歴情報を参照するステップと、サーバに蓄積されている電子メールの送信履歴に係る送信履歴情報を参照するステップと、依頼履歴情報と送信履歴情報とを比較するステップと、比較結果に基づいて動作異常を検出するステップとを実行させることができる。

【００２７】

コンピュータのハードディスクに本発明のプログラムをインストールすることにより、コンピュータ側で依頼履歴情報と送信履歴情報との比較処理を行うことができる。そのため、サーバの処理に頼ることなく、ユーザの好きなときにウイルス存在の有無をチェックすることができる。また、本発明の異常検出方法は、電子メールの送信時だけでなく定期的にウイルス存在の有無をチェックするようにしてもよい。

【００２８】

また、本発明は、電子メールの送信を依頼するコンピュータに電子メール送信

サービスを提供するサーバであってもよい。

本発明のサーバは、コンピュータから電子メールの送信依頼を受け付ける受付手段と、送信依頼を受けた電子メールを送信する送信手段と、送信した電子メールに係る送信履歴情報を蓄積する蓄積手段と、コンピュータに蓄積されている電子メールの送信依頼履歴に係る依頼履歴情報をコンピュータから参照する履歴参照手段と、送信履歴情報と依頼履歴情報とを比較する比較手段と、比較結果に基づいてコンピュータの動作異常を検出する検出手段とを備えることを特徴とする。

【００２９】

さらに、本発明は、電子メール送信サービスを提供するサーバに電子メールの送信を依頼するコンピュータであってもよい。

本発明のコンピュータは、サーバに電子メールの送信を依頼する依頼手段と、送信を依頼した電子メールに係る依頼履歴情報を蓄積する蓄積手段と、サーバに蓄積されている電子メールの送信履歴に係る送信履歴情報をサーバから参照するサーバ履歴参照手段と、依頼履歴情報と送信履歴情報とを比較する比較手段と、比較結果に基づいて動作異常を検出する検出手段とを備えることを特徴とする。

【００３０】

【発明の実施の形態】

以下、本実施形態における異常検出システム及び異常検出方法について説明する。

【００３１】

＜第一の実施の形態＞

（発明の概要）

図１に、本実施形態におけるメール送信システム１の概念図を示す。本実施形態における電子メール（以下、メールと称す）２の送信は、ユーザ端末（以下、メールクライアントと称す）３のメールソフト４を利用して行われる。

【００３２】

このとき、メールクライアント３は、送信したメール２に関する様々な履歴データ（依頼履歴情報に相当、以下依頼履歴データと称す）をメールクライアント

３内に蓄積する。依頼履歴データとしては、送信先のアドレス、送信日時、送信したメールのタイトルや添付ファイルの有無等を例示できる。

【００３３】

メールクライアント３から送信されたメール２は、サーバ（以下、メールサーバと称す）５を中継し送信先に配信される。メールサーバ５は、送信依頼を受けたメール２を送信先の端末に送信する。メールサーバ５は、このメール２を送信したときに、前記メール２に関する送信履歴データ（送信履歴情報に相当する）をメールサーバ５内のデータベースに蓄積する

【００３４】

このとき、メールクライアント３が蓄積した依頼履歴データと、メールサーバ５が蓄積した送信履歴データとは同一のメールに関する情報を含む。本実施形態では、このような構成によりメールの送信が行われる。

【００３５】

そして、本実施形態の異常検出方法では、上述したようにメールの送信が行われた時に、ウイルスがそのメールを送信した事実はあるかを検出する。

【００３６】

図２に本実施形態のウイルスが独自にメールを送信した場合の概念図を示す。本実施形態のウイルスはメールを独自に送信する機能（メールエンジン）を有しているとする。

【００３７】

上述したように、メールソフト４によりメールを送信するとそのメールの依頼履歴データがメールクライアント３に蓄積される。一方、ウイルスが独自のメールエンジンでメールを送信した場合、メールソフト４を利用せずにメールが送信されている為、送信されたメールの依頼履歴データはクライアント端末３には蓄積されない。

【００３８】

しかし、ウイルスによって送信依頼されたメールもメールサーバ５を経由して送信先に送信される。そのため、ウイルスによって送信を依頼されたメールはメールサーバ５を一度経由する。ここでメールサーバ５は、ウイルスによって送信

されたメールを送信先に送信したときに、そのメールの送信履歴データを蓄積する。

【００３９】

そして、メールサーバ５は、メールクライアント３に記録された依頼履歴データと、メールサーバ５に記録された送信履歴データとを比較する。これによって、メールクライアント３の依頼履歴データにないメールの送信履歴データがメールサーバ５にある場合、このメールを送信したメールクライアント３はウイルスに感染している可能性が高いということがわかる。

【００４０】

次に、本実施形態におけるメールクライアント３とメールサーバ５とのシステム構成を説明する。

【００４１】

（システム構成）

図３に本実施形態におけるメールクライアント３とメールサーバ５のシステム構成図を示す。

【００４２】

まず、本実施形態のメールクライアント３について説明する。メールクライアント３は、メールクライアント３全体の制御を行うＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）と、ＣＰＵにて実行される基本プログラムを格納したＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）と、ＣＰＵで実行されるオペレーティングシステム，各種アプリケーション，各種データを格納したＨＤ（Ｈａｒｄ　Ｄｉｓｋ）と、ＣＰＵで実行されるプログラムやＣＰＵでの処理データを一時的に記憶するＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）と、ネットワークを介してデータの送受信を行う為の通信インターフェースと、ユーザが外部から各種データを入力するための入力インターフェースとを有する既存のパーソナルコンピュータであるとする（何れも図示せず）。

【００４３】

本実施形態のメールクライアント３には、メールソフト４がインストールされている。このメールソフト４は、メールクライアント３から本アプリケーション

を操作するためのユーザインターフェース６と、メールを送信する為のメール送信エンジン７ａとを有している。

【００４４】

また、メールクライアント３のＨＤには、複数の依頼履歴データのファイルが格納されている。これらの依頼履歴データファイルには、メールの送信条件データが格納された送信条件データファイル８ａと、メールソフト４の動作履歴が格納された動作履歴データファイル９と、メールを送信したときの依頼履歴データファイル１０ａとがある。これらのファイルはＨＤ内に構築されている。尚、これらの履歴データについては後述する。

【００４５】

さらに、メールソフト４は、比較必要条件設定プログラム１１を有している。比較必要条件設定プログラム１１は、メールの送信に関する条件パラメータを予め設定し、送信条件データファイル８ａに格納する為のプログラムである。尚、比較必要条件設定プログラム１１により設定する各種データについては後述する。

【００４６】

また、メールソフト４は、設定した条件と実際にファイルに格納したデータとの比較を行う比較必要条件チェックプログラム１２ａを有している。

【００４７】

次に、本実施形態のメールサーバ５について説明する。メールサーバ５も、メールクライアント３と同様に、メールサーバ５全体の制御を行うＣＰＵと、ＣＰＵで実行される基本プログラムを格納するＲＯＭと、ＣＰＵで実行されるオペレーティングシステム，各種アプリケーション，各種データを格納するＨＤと、ＣＰＵでの処理内容を一時的に記録するＲＡＭと、ネットワークを介してデータの送受信を行う為の通信インターフェースとを備える既存のコンピュータであるとする（何れも図示せず）。

【００４８】

さらに、メールサーバ５はメール送信エンジン７ｂを有している。加えて、メールサーバ５のＨＤには、メールクライアント３から送信された送信条件データ

を格納する送信条件データファイル８ｂと、メールクライアント３から送信依頼されたメールを送信先に送信したときの送信履歴データを格納する送信履歴データファイル１０ｂと、比較必要条件チェックプログラム１２ｂとを省略する。

【００４９】

その他に、本実施形態のメールサーバ５のＨＤには、メールクライアント３に格納されている依頼履歴データとメールサーバ５に格納された送信履歴データとを比較する履歴チェックプログラム１３がインストールされている。

【００５０】

また、本実施の形態のメールサーバ５及びメールクライアント３は、例えば、電子メールの送信用の通信プロトコルとしてＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｅａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、電子メールの受信用の通信プロトコルとしてＰＯＰ（Ｐｏｓｔ　Ｏｆｆｉｃｅ　Ｐｒｏｔｏｃｏｌ）を利用する。尚、既知の他のプロトコルを利用するものであっても良いことはいうまでもない。

【００５１】

以上が、本実施形態におけるメールクライアント３及びメールサーバ５のシステム構成である。

【００５２】

（データ構造）

次に、メールクライアント３の依頼履歴データファイル１０ａに格納する依頼履歴データについて説明する。

【００５３】

図４にメールクライアント３に蓄積される依頼履歴データの一覧を示す。メールクライアント３に蓄積される依頼履歴データは、メールサーバ５に送信したメール全体の履歴に関するデータと、各メールの履歴に関するデータとに分類される。

【００５４】

メール全体の依頼履歴データには、メールサーバ５に送信したメールの総数と、最も古いメールの送信日時と、最も新しいメールの送信日時と、最新のウイルス定義情報（パターンファイル）を受信した日時が含まれる。

【００５５】

各メールの依頼履歴データには、送信したメールの題名と、メールの送信をした送信元のアドレスと、メール送信先のアドレスと、添付ファイルの有無と、添付ファイル名と、送信したメールの本文と、送信日時と、送信したメールのヘッダーとが含まれる。

【００５６】

次に、メールサーバ５の送信履歴データファイル１０ｂに格納する送信履歴データについて説明する。

【００５７】

図５にメールサーバ５に蓄積される送信履歴データの一覧を示す。メールサーバ５に蓄積される送信履歴データは、メールクライアント３から送信依頼され、送信したメール全体に関する送信履歴データと、各メールに関する送信履歴データとに分類される。

【００５８】

メール全体に関する送信履歴データには、メールクライアント３から送信依頼されて送信したメールの総数と、最も古いメールの送信日時と、最も新しいメールの送信日時とが含まれている。

【００５９】

各メールの送信履歴データには、送信したメールの題名と、メールの送信元のアドレスと、メールの送信先のアドレスと、添付ファイルの有無と、添付ファイル名と、メールの本文と、メールクライアント３からメールの送信依頼を受け付けた受付日時（受信時間）と、メールを送信先に送信した送信日時と、メールのヘッダーと、メールクライアント３からの送信経路情報とが含まれる。

【００６０】

以上が、メールクライアント３及びメールサーバ５で蓄積される依頼履歴データ及び履歴データの説明である。比較必要条件設定プログラム１１は、上述した依頼履歴データと送信履歴データとを比較する（以下、「履歴を比較する」という）時の条件を設定するプログラムである。

【００６１】

そこで次に、比較必要条件設定プログラム１１による条件の設定例の説明を行う。

【００６２】

図６に比較必要条件設定プログラム１１による設定内容の一覧を示す。まず、この一覧の項目の説明をする。

【００６３】

図６中Ｌ１に示す項目は、「前回履歴を比較した日時」の項目である。前回履歴比較を行った日時は、前回履歴比較プログラムにより依頼履歴データと送信履歴データの比較が行われた際に記録されることとする。

【００６４】

図６中Ｌ２に示す項目は、「前回の比較日時からどれだけ経過したら比較するか」の項目である。この項目は、Ｌ１の項目中の日時を基点としユーザにより設定することができる。例えば、前回履歴を比較した日時から二週間後毎に履歴の比較を行うというように、ユーザは条件を設定することができる。

【００６５】

図６中Ｌ３に示す項目は、「最新ウイルス情報を受け取ってから比較をしたか」という項目である。つまり、最新ウイルス情報を受け取った日時の方がＬ１の項目中の日時よりも前の日時である場合、最新ウイルス情報を受け取ってから履歴の比較が行われたということになる。

【００６６】

図６中Ｌ４に示す項目は、「一定時間内のメール送信数：クライアントが許可している数」という項目である。この項目は、メールクライアント３が一定時間に送信されるメールの上限数を設定する項目である。

【００６７】

図６中Ｌ５に示す項目は、「一定時間内のメール送信数：今までの最大送信数」という項目である。この項目は、メールクライアント３から一定時間内にメールが送信される度に記録されることとする。そして、これまでの最大送信数を超える送信数がカウントされると最大送信数を更新するようにする。

【００６８】

図６中Ｌ６に示す項目は、「同じ内容のメール送信数：メールクライアント３が許可している数」という項目である。これは、メールクライアント３が送信する同報メールの送信数の上限を設定する為の項目である。

【００６９】

図６中Ｌ７に示す項目は、「同じ内容のメール送信数：今までの最大送信数」という項目である。この項目の最大送信数は、これまでの最大送信数を超える送信数がカウントされると最大送信数を更新するようにすると好ましい。

【００７０】

図３に示すように、上述した設定内容は、送信条件データとしてメールクライアント３の送信条件データファイル８ａに蓄積される。また、後述するが送信条件データは、メールクライアント３からメールサーバ５に送信される。そのため、送信条件データはメールサーバ５の送信条件データファイル８ｂにも蓄積される。

【００７１】

次に、メールクライアント３の動作履歴データファイル９に格納される、メールソフト４の動作履歴データについて説明する。

【００７２】

図７に動作履歴データの一覧を示す。動作履歴データには、メールソフト４を利用して送信したメール全体に関する履歴と、メールソフト４の起動に関する履歴と、メールの送信先／送信元に関する履歴と、メールサーバ５に送信した各々のメールに関する履歴とが含まれる。

【００７３】

メールソフト４を利用して送信したメール全体に関する履歴には、動作記録を取得したメールの総数と、最も古いメールの送信を依頼したときのメールソフト４の動作日時と、最新のメールの送信を依頼したときのメールソフト４の動作日時とが含まれている。

【００７４】

メールソフト４の起動に関する履歴には、メールソフト４の起動日時と、メールソフト４の起動終了日時と、メールソフト４起動中に送信を行ったメール数と

を含む。

【００７５】

メールの送信先に関する履歴には、送信先のアドレスと、その送信先に今まで送信されたメールの総数と、その送信先に前回メールを送信した日時とを含む。尚、メールの送信元に関する履歴には、メールクライアント３が使用しているメールソフトの種類やメールアドレス等が含まれる。

【００７６】

メールサーバ５に送信を依頼した各々のメールに関する履歴には、送信を依頼したメールの題名と、題名の入力方法と、送信元のメールアドレスと、送信先のメールアドレスと、送信先の選択方法のデータが含まれる。題名の入力方法は、ユーザが任意の題名をキーボード等から直接入力した場合と、返信時に自動的に付与される「Ｒｅ＋受信したメールの題名」が題名となり題名を特別に入力する必要がない場合とにより異なる。また、送信先の選択方法には、ユーザがキーボード等の入力インターフェースにより選択先のアドレスを直接入力する方法と、ユーザがマウス等により選択先のアドレスをメールソフト４に搭載されたアドレス帳から選択する方法とがある。

【００７７】

また、メールサーバ５に送信を依頼した各々のメールに関する履歴には、メールの作成方法と、添付ファイルの有無と、添付ファイル名と、添付ファイルの選択方法とが含まれている。メールの作成方法とは、新規作成，返信，転送といったメールの種類のことである。また、添付ファイル名は、カンマやセミコロン等で区切る等して複数名記録できると好ましい。

【００７８】

その他に、メールクライアント３がメールサーバ５に送信を依頼した各々のメールに関する履歴には、メール本文の内容と、本文入力の有無と、メール送信をした日時と、送信を決定する処理の有無と、送信を決定する処理が行われた画面／部品名の履歴と、メール送信後の送信経過ダイアログの表示の有無とを含む。

【００７９】

本文入力の有無とは、ユーザがキーボード等の入力インターフェースから直接

本文を入力した場合は本文入力有り、転送・コピー等により本文を作成した場合は本文入力無しということを意味する。

【００８０】

送信決定処理の有無とは、メールの送信を決定する為の処理が有るか否かを意味する。この、送信決定処理は、「メールの送信」というようなアイコンやメニューから実行する等の処理方法を例示できる。

【００８１】

送信を決定する処理が行われた画面／部品名の履歴とは、送信決定処理が画面に設けられたアイコン（ボタン）から行われたか、メニュー画面から行われたかという内容の履歴である。

【００８２】

以上が、メールクライアント３の動作履歴データファイル９内に蓄積される動作履歴データの説明である。

【００８３】

（異常検出処理手順）

以下、本実施形態の異常検出手順を説明する。

【００８４】

図８に本実施形態における異常検出手順のフローチャートを示す。

【００８５】

まず、メールクライアント３のＣＰＵは比較必要条件設定プログラム１１を実行する。ここで、ユーザは、比較必要条件設定プログラム１１に従い送信条件データの設定を行う（Ｓ０１）。この設定は、図５に示す設定内容を設定する。例えば、「前回の比較日時からどれだけ経過したら比較するか」の項目を二週間、「一定時間のメール送信数」の項目を５０通、「同じ内容のメール送信数」の項目を１０通と設定する。

【００８６】

そして、ユーザにより設定された送信条件データは、メールクライアント３の送信条件データファイル８ａに蓄積される。

【００８７】

比較必要条件設定プログラム１１は、送信条件データの設定完了を受けて、ユーザにより入力された送信条件データをメールサーバ５に送信する。送信条件データの送信完了を受けて比較必要条件設定プログラム１１は終了する。

【００８８】

設定内容を受信したメールサーバ５は、設定内容を送信条件データファイル８ｂに保存する（Ｓ０２）。

【００８９】

一方、メールクライアント３は、ユーザによるメールの送信操作を検出すると、そのメールの送信をメールサーバ５に送信を依頼する（Ｓ０３）。

【００９０】

メールの送信依頼に伴い、メールクライアント３のＣＰＵは、当該メールの依頼履歴データを作成し、所定のファイルに蓄積する（Ｓ０４）。ここで作成された依頼履歴データは、前述した図４に示す依頼履歴データと図７に示す動作履歴データとを含む。

【００９１】

依頼履歴データの蓄積が完了すると、メールクライアント３のＣＰＵは比較必要条件チェックプログラム１２ａを実行する。比較必要条件チェックプログラム１２ａは、比較必要条件設定プログラム１１により設定された図６に示す送信条件データと、蓄積した依頼履歴データとの比較処理を行う（Ｓ０５）。

【００９２】

すなわち、比較必要条件チェックプログラム１２ａは、送信条件データと送信したメールに関する依頼履歴データに基づき、前回の比較日時から所定の日数（例えば、二週間）が経過しているか否か、最新ウイルス情報を受けとってから比較処理を行ったか否か、一定時間内のメール送信数は設定値（例えば、５０通）を超えているか否か、同じ内容のメール送信数が設定値（例えば、１０通）を超えているか否かという項目について比較処理を行う。

【００９３】

ここで、図４に示す依頼履歴データが図６に示す送信条件データを満たした場合、比較必要条件チェックプログラム１２ａは、さらに詳細なチェックを実行す

る。すなわち、比較必要条件チェックプログラム１２ａは、メールクライアント３が蓄積した依頼履歴データとメールサーバ５が蓄積した送信履歴データとを比較する。尚、比較必要条件チェックプログラム１２ａは、上述した項目全てを満たさなければならないという判断を行ってもよいが、重要度の高い項目を満たしていなければ問題が無いという判断を行うようにしてもよい。例えば、一定時間内のメール送信数が設定数を超えている場合や、同一内容のメールが設定数を送信されている場合などはウイルスによるメールの送信である可能性が高いため重要度が高い項目といえる。

【００９４】

ステップ０５で比較必要条件チェックプログラム１２ａが、図４に示す依頼履歴データが図６に示す送信条件データを満たしていないと判断した場合、メールサーバ５から送信履歴データの要求の有無を確認する（Ｓ０６）。

【００９５】

ここで、比較必要条件チェックプログラム１２ａが、メールサーバ５から依頼履歴データの要求は無いと判断した場合、ステップ０３に戻り同様の処理を繰り返す。一方、比較必要条件チェックプログラム１２ａが、メールサーバ５から依頼履歴データの要求があると判断した場合は、依頼履歴データをメールサーバ５に送信する（Ｓ０７）。

【００９６】

一方、比較必要条件プログラム１２ａが、依頼履歴データは送信条件データを満たしていると判断した場合、比較必要条件チェックプログラム１２ａは蓄積した依頼履歴データをメールサーバ５に送信する（Ｓ０７）。

【００９７】

また、ステップ０２で、メールクライアント３からメール送信依頼を受けたメールサーバ５は、メールクライアント３から送信依頼されたメールを受理する（Ｓ０８）。メールサーバ５は、送信依頼のあったメールの受理を確認した後、送信先へメールを送信する。

【００９８】

メールサーバ５のＣＰＵは、メールの送信と共に、送信したメールに関する送

信履歴データを所定のファイルに蓄積する（Ｓ０９）。尚、ここでの送信履歴データとは、前述した図５に示す送信履歴データのことである。

【００９９】

メールサーバ５のＣＰＵは送信履歴データを蓄積したことを受けて、比較必要条件チェックプログラム１２ｂを実行する（Ｓ１０）。比較必要条件チェックプログラム１２ｂは、メールサーバ５が蓄積した送信履歴データとステップ０２でメールクライアント３から送信された送信条件データとを比較する。尚、比較項目についてはメールクライアント３における比較必要条件チェックプログラム１２ａの比較項目と同じであるため説明を省略する。

【０１００】

ステップ１０で比較必要条件チェックプログラム１２ｂが送信履歴データが送信条件データを満たしていないと判断した場合、ステップ０８に戻り同様の処理を繰り返す。

【０１０１】

一方、ステップ１０で送信履歴データが送信条件データを満たしたと判断した場合、比較必要条件チェックプログラム１２ｂはメールクライアント３に依頼履歴データの送信要求処理を行う（Ｓ１１）。

【０１０２】

メールクライアント３から送信された依頼履歴データを受信したことを受けて、メールサーバ５のＣＰＵは、履歴チェックプログラム１３を実行する（Ｓ１２）。

【０１０３】

履歴チェックプログラム１３は、図４に示すメールクライアント３が蓄積した依頼履歴データと図５に示すメールサーバ５が蓄積した送信履歴データとを比較する。

【０１０４】

以下の比較例では、メールサーバがメールクライアントから送信依頼を受けて送信したメールは、メールサーバ５が送信依頼を受けた日時（受付日時）の前後から所定時間以内（例えば１０分間）にメールクライアント３が送信依頼したメ

ールと同一であることを前提とする。尚、受付日時に代えて送信日時を用いてもよい。

【０１０５】

また、メールクライアントが送信依頼したメールと、メールサーバが送信依頼を受けたメールが同一か否かは、図４及び図５に示す送信元（ホスト名、ＩＰアドレス等）から判定する。尚、以下に示す比較処理を全て実施することで異常なメール送信を検出する割合が高くなるが、必ずしもこれに限定されるものではなく、適宜選択又は組み合わせて実施するようにすればよい。

【０１０６】

さらに、メールクライアントが送信依頼したメールと、メールサーバが送信依頼を受けたメールが同一か否かは、最新の依頼履歴データと最新の送信履歴データとを比較して判定してもよい。

【０１０７】

（比較例１）

履歴チェックプログラム１３は、メールサーバ５がメールクライアント３からの依頼により蓄積した送信履歴データ中の最も新しいメールの送信日時と、メールクライアント３が蓄積した依頼履歴データ中の最も新しいメールの送信日時とを比較する。依頼履歴データ中に、上記送信日時に近い時間帯のメール送信がない場合、メールクライアント３はメールサーバ５が送信依頼を受けたメールを送信依頼していないことになる。つまり、メールサーバ５が送信依頼を受けたメールはウイルスが送信したメールである可能性が高いということなる。

【０１０８】

（比較例２）

履歴チェックプログラム１３は、メールサーバ５がメールクライアント３からの依頼により蓄積した最新の送信履歴データ中のメールの題名と、メールクライアント３が蓄積した依頼履歴データ中のメールの題名とを比較する。依頼履歴中にメールサーバ５が送信したメールの題名がない場合、メールサーバ５が送信依頼を受けたメールはメールクライアント３が送信を依頼したものではないことがわかる。つまり、メールサーバ５が送信依頼を受けたメールはウイルスが送信し

たメールである可能性が高いということになる。

【０１０９】

（比較例３）

比較履歴チェックプログラム１３は、メールサーバ５が蓄積した送信履歴データ中のメールの総数（メールクライアント３から送信依頼されて送信したメールの総数）と、メールクライアント３が蓄積した依頼履歴データ中のメールの総数（サーバに送信依頼したメールの総数）とを比較する。双方のメールの総数は異なる場合、メールサーバ５が送信依頼を受けたメールはメールクライアント３が送信を依頼したものではないことがわかる。つまり、メールサーバ５が送信依頼を受けたメール中にはウイルスが独自の送信エンジンを用いてメールを送信している可能性が高いと考えられる。

【０１１０】

（比較例４）

比較履歴チェックプログラム１３は、メールクライアント３からの最新の送信依頼メールに関する送信履歴データ中の送信元に関するデータと、メールクライアント３が蓄積した依頼履歴データ中の送信元に関するデータとを比較する。尚、送信元に関するデータは、送信元のメールアドレス、ユーザ名等ユーザを特定する各種情報を含む。双方の送信元のメールアドレスは異なる場合、メールサーバ５が送信依頼を受けたメールはメールクライアント３が送信を依頼したものではないことがわかる。つまり、上記最新の送信依頼メールは、ウイルスが独自の送信エンジンを用いて送信したメールである可能性が高いと考えられる。

【０１１１】

（比較例５）

比較履歴チェックプログラム１３は、メールクライアント３からの依頼により蓄積した送信履歴データ中の最新メールの本文データと、メールクライアント３が蓄積した依頼履歴データ中の最新メールの本文データとを比較する。メールサーバ５に蓄積された本文データがメールクライアント３に蓄積された本文データにない場合或いは本文データの内容が異なる場合、メールサーバ５が送信依頼を受けたメールはメールクライアント３が送信を依頼したものではないことがわか

る。つまり、メールサーバ５が送信依頼を受けたメールはウイルスが独自の送信エンジンを用いて送信したものである可能性が高いと考えられる。尚、メールの本文が長文の場合、メールの本文データを依頼履歴データ及び送信履歴データとは別のデータとして管理しても良い。

【０１１２】

（比較例６）

比較履歴チェックプログラム１３は、メールサーバ５が蓄積した送信履歴データ中のメールクライアント３から送信依頼を受けた最新メールのヘッダーと、メールクライアント３が蓄積した依頼履歴データ中の最新のメールのヘッダーとを比較する。これによって、一方のヘッダーは「Ｆｗｄ（転送）」であり他方のヘッダーは「Ｒｅ（返信）」というように異なる場合、或いはメールクライアント３に蓄積された最新メールのヘッダーがメールサーバ５に蓄積された最新メールのヘッダーにない場合、メールサーバ５が送信依頼を受けたメールは、メールクライアント３が送信を依頼したメールではないことがわかる。つまり、メールサーバ５が送信依頼を受けたメールはウイルスにより独自の送信エンジンを用いて送信された可能性が高いと考えられる。

【０１１３】

（比較例７）

比較履歴チェックプログラム１３は、メールサーバ５が蓄積した送信履歴データ中の最も古いメールの送信依頼受け日時と、メールクライアント３が蓄積した依頼履歴データ中の最も古いメールの送信日時とを比較する。尚、両者の送信日時の保持期間（例えば一ヶ月）は同じであるとする。双方の日時は異なるという比較結果の場合、メールサーバ５が送信依頼を受けたメールとメールクライアント３が送信を依頼したものではないことがわかる。つまり、メールサーバ５が送信依頼を受けたメールはウイルスが独自の送信エンジンを用いてメールを送信した可能性が高いと考えられる。尚、この比較は、ウイルスに感染している可能性があるか否かの現状を最新でチェックするというより、定期的に比較を行う場合に適している。

【０１１４】

（比較例８）

比較履歴チェックプログラム１３は、メールサーバ５がメールクライアント３から依頼を受けて蓄積した送信履歴データ中の最新メールにおける添付ファイル名と、メールクライアント３が蓄積した依頼履歴データ中の最新メールにおける添付ファイル名とを比較する。メールサーバ５に蓄積された最新メールの添付ファイル名が、メールクライアント３の依頼履歴データ中にない場合、メールサーバ５が送信依頼を受けたメールはメールクライアント３が送信を依頼したものではないことがわかる。つまり、メールサーバ５が送信依頼を受けたメールはウイルスが送信したメールである可能性が高いということになる。

【０１１５】

（比較例９）

比較履歴チェックプログラム１３は、メールサーバ５がメールクライアント３から依頼を受けて蓄積した送信履歴データ中の最新メールにおける添付ファイルの有無に関するデータと、メールクライアント３が蓄積した依頼履歴データ中の最新メールにおける添付ファイルの有無に関するデータとを比較する。メールサーバ５が送信依頼を受けたメールには添付ファイルがあり、メールクライアント３が送信依頼をしたメールには添付ファイルがない場合、メールサーバ５が送信依頼を受けたメールはメールクライアント３が送信を依頼したメールではないことがわかる。つまり、メールサーバ５が送信依頼を受けたメールはウイルスにより独自に送信されたメールである可能性が高いと考えられる。

【０１１６】

（比較例１０）

比較履歴チェックプログラム１３は、メールサーバ５がメールクライアント３からの依頼を受けて蓄積した送信履歴データ中の最新メールにおける送信先に関するデータと、メールクライアント３が蓄積した依頼履歴データ中の最新メールにおける送信先に関するデータとを比較する。尚、送信先に関するデータは、送信先のメールアドレスやユーザ名等、送信先を特定する情報を含む。送信先に関する双方のデータは異なる場合、或いはメールサーバ５に蓄積された送信履歴データ中の送信先がメールクライアント３に蓄積された依頼履歴データ中の送信先

にない場合、メールサーバ５が送信依頼を受けたメールはメールクライアント３が送信を依頼したものではないことがわかる。つまり、メールサーバ５が送信依頼を受けたメールはウイルスにより独自に送信されたメールである可能性が高い。

【０１１７】

（比較例１１）

履歴チェックプログラム１３は、メールサーバ５がメールクライアント３からの依頼を受けて蓄積した送信履歴データと、メールクライアント３が蓄積した動作履歴データとを比較する。図７に示すように動作履歴データには、メールソフトの起動時間，終了時間，送信先のアドレス，送信元のアドレス，メールの題名，添付ファイルの有無，添付ファイル名，メール本文の内容等が含まれる。

【０１１８】

例えば、メールサーバ５が蓄積した送信履歴データ中のメールの送信依頼を受けた受付日時（図５中受信日時）と、メールクライアント３が蓄積した動作履歴データ中のメールソフトの起動時間（図７中起動日時）とを比較する。メール送信依頼を受けた受付日時は起動時間内に含まれていないという比較結果の場合、そのメールはメールソフトから送信されたものではない。つまり、メールサーバ５が送信依頼を受けたメールは、ウイルスが独自のメール送信エンジンによって送信したメールである可能性が高いということになる。

【０１１９】

また、履歴比較チェックプログラム１３は、メールサーバ５が蓄積した送信履歴データ中のメールの送信依頼を受けた受付日時（図５中受信日時）と、メールクライアント３が蓄積した動作履歴データ中のメールソフトの起動終了時間（図７中終了時間）とを比較する。受付時間が起動終了時間よりも後であるという比較結果の場合、メールサーバ５に送信を依頼されたメールはメールソフトから送信されたものではない。つまり、メールサーバ５が送信依頼を受けたメールは、ウイルスが独自のメール送信エンジンによって送信したメールである可能性が高いということになる。

【０１２０】

さらに、履歴比較チェックプログラム１３は、

（１）メールサーバ５が蓄積した送信履歴データ中におけるメールの送信先のアドレスと、メールクライアント３が蓄積した動作履歴データ中における送信先のアドレスとの比較，

（２）メールサーバ５が蓄積した送信履歴データ中における送信元のアドレスと、メールクライアント３が蓄積した動作履歴データ中における送信元のアドレスとの比較，

（３）メールサーバ５が蓄積した送信履歴データ中におけるメールの題名と、メールクライアント３が蓄積した動作履歴データ中におけるメールの題名との比較，

（４）メールサーバ５が蓄積した送信履歴データ中におけるメール本文の内容と、メールクライアント３が蓄積した動作履歴データ中におけるメール本文の内容との比較，

（５）メールサーバ５が蓄積した送信履歴データ中における添付ファイルの有無と、メールクライアント３が蓄積した動作履歴データ中における添付ファイルの有無との比較，

（６）メールサーバ５が蓄積した送信履歴データ中における添付ファイル名と、メールクライアント３が蓄積した動作履歴データ中における添付ファイル名との比較、

を行ってもよい。何れも、上述したメールクライアント３が蓄積した依頼履歴データ中にある各項目と同じであり、依頼履歴データと動作履歴データとの比較により双方の最新メールの同一性、又は一致するメールの存在の有無を調べる。最新メール同士の同一性が見られない場合、又は一致するメールが存在しない場合は、ウイルスが送信したものがある可能性が高いということになる。

【０１２１】

そして、ステップ１２で、履歴チェックプログラム１３が双方のデータに相違は無いと判断した場合、ステップ０８に戻り同様の処理を繰り返す。つまり、メールサーバ５が送信依頼を受けたメールと、メールクライアント３が送信したメールは同一であるとき、ウイルスに感染している可能性は低いとみなされる。

【０１２２】

一方、履歴チェックプログラム１３が双方のデータに差異があると判断した場合、ウイルスに感染している可能性が高いと考えられる。そこで、履歴チェックプログラム１３は、ウイルスに感染している可能性が高いという旨をメールクライアント３に通知する（Ｓ１３）。

【０１２３】

この通知を受けたメールクライアント３のＣＰＵは、メールクライアント３のディスプレイにウイルス感染した可能性がある旨を表示する（Ｓ１４）。

【０１２４】

以上の手順を経ることにより、メール送信を実行するウイルス存在の可能性を検出することができる。

【０１２５】

本実施形態における異常検出方法によれば、自身がメール送信機能（メール送信エンジン）を有し無秩序にメールを送信するタイプのウイルスの存在を検出することができる。

【０１２６】

上記実施形態では、メールサーバ５の送信履歴データとメールクライアント３の依頼履歴データとを比較してウイルスの存在を検出した。しかし、本発明の実施は、このような構成には限定されない。例えば、送信条件データと依頼履歴データとを比較することによりウイルス存在の有無を検出するようにしてもよい。例えば、長期間送信していないあて先の送信や、所定時間あたり所定数を超えるメールの送信等をチェックすることによってウイルス存在の有無を検出する。これによって、本実施形態における異常検出方法によれば、自身がメール送信機能を有さずメールクライアントのメールソフトを利用してメールを送信するタイプのウイルスの何れのタイプのウイルスにも対応することができる。

【０１２７】

また、本実施形態における異常検出システム・方法は、メールの送信履歴及びメールソフトの動作履歴と過去の履歴とを比較することによりウイルス感染の可能性の検出を行う。そのため、ウイルスチェックソフトを導入していないメール

クライアントにおいても、対応するウイルス定義情報が更新されていないメールクライアントにおいても、ウイルスのメール送信の事実を摘出することができる。

【０１２８】

また、履歴チェックプログラムがメールサーバで実行されることにより、メールクライアントで実行しなければならないプログラムの数を抑えることができる。すなわち、本実施形態の異常検出システムによれば、メールクライアントの端末自体のスペックに左右されることなく送信履歴のチェックを行い、ウイルスの存在を確認することができる。

【０１２９】

＜第二の実施の形態＞

本実施形態の異常検出システム・方法は、メールクライアント３に蓄積された依頼履歴データとメールサーバ５に蓄積された送信履歴データとの比較をメールクライアント３側で行う。

【０１３０】

図９に本実施形態におけるメールクライアント３及びメールサーバ５のシステム構成図を示す。図９に示すように、本実施形態のメールクライアント３は、履歴チェックプログラム１３を有している。尚、本実施形態のメールサーバ５及びメールクライアント３の構成，蓄積するデータの内容，データの比較項目は第一の実施の形態と同一であるので、重複する説明は省略する。加えて、図面中において第一の実施の形態と同一の部位には同一の符号を付した。

【０１３１】

以下に、本実施形態における異常検出手順を説明する。

【０１３２】

図１０に本実施形態における異常検出手順のフローチャートを示す。

【０１３３】

まず、メールクライアント３のＣＰＵは比較必要条件設定プログラム１１を実行する。ここで、ユーザは、比較必要条件設定プログラム１１に従い送信条件データの設定を行う（Ｓ１００）。この設定は、第一の実施の形態と同様に図５に

示す設定内容を設定する。

【０１３４】

そして、ユーザにより設定された送信条件データは、メールクライアント３の送信条件データファイル８ａに蓄積される。

【０１３５】

比較必要条件設定プログラム１１は、送信条件データの設定完了を受けて、ユーザにより入力された送信条件データをメールサーバ５に送信する。送信条件データの送信完了を受けて比較必要条件設定プログラム１１は終了する。

【０１３６】

設定内容（送信条件データ）を受信したメールサーバ５は、設定内容を送信条件データファイル８ｂに保存する（Ｓ１０１）。

【０１３７】

一方、メールクライアント３では、メール送信を決定する処理が行われた上でメールサーバ５にメールを送信する。即ち、メールクライアント３からメールを送信する（Ｓ１０２）。

【０１３８】

メールクライアント３からメールを受けたメールサーバ５は、メールクライアント３から送信されたメールを受け付ける（Ｓ１０３）。メールサーバ５は、メールの受理を確認した後、送信先へメールを送信する。

【０１３９】

メールサーバ５のＣＰＵは、メールの送信と共に、当該メールの送信履歴データを所定のファイルに蓄積する（Ｓ１０４）。尚、ここでの送信履歴データとは、第一の実施の形態と同じく図５に示す送信履歴データのことである。

【０１４０】

メールサーバ５のＣＰＵは、送信履歴データを蓄積したことを受けて、比較必要条件チェックプログラム１２ｂを実行する（Ｓ１０５）。比較必要条件チェックプログラム１２ｂは、メールサーバ５自身が蓄積した送信履歴データとステップ１０１でメールクライアント３から送信された送信条件データとを比較する。

【０１４１】

比較必要条件チェックプログラム１２ｂは、送信条件データと送信履歴データを、前回の比較日時から所定の日数（例えば、二週間）が経過しているか否か、最新ウイルス情報を受けてとってから比較処理を行ったか否か、一定時間内のメール送信数は設定値（例えば、５０通）を超えているか否か、同じ内容のメール送信数が設定値（例えば、１０通）を超えているか否かという項目について比較処理を行う。

【０１４２】

ステップ１０５で比較必要条件チェックプログラム１２ｂが、送信履歴データは送信条件データを満たしていないと判断した場合、メールクライアント３から依頼履歴データの送信要求の有無を確認する（Ｓ１０６）。

【０１４３】

ここで、比較必要条件チェックプログラム１２ｂが、メールクライアント３から送信履歴データの送信要求が無いと判断した場合、ステップ１０３に戻り同様の処理を繰り返す。

【０１４４】

一方、比較必要条件チェックプログラム１２ｂが、メールクライアント３から送信履歴データの送信要求があると判断した場合は、送信履歴データをメールクライアント３に送信する（Ｓ１０７）。

【０１４５】

また、ステップ１０５で、比較必要条件チェックプログラム１２ｂが、送信履歴データは送信条件データを満たしていると判断した場合、メールクライアント３が蓄積した依頼履歴データとメールサーバ５が蓄積した送信履歴データとを比較する必要があるということになる。

【０１４６】

すると、比較必要条件チェックプログラム１２ｂは蓄積した送信履歴データをメールクライアント３に送信する（Ｓ１０７）。

【０１４７】

また、メールクライアント３のＣＰＵは、ステップ１０２で、メールサーバ５にメールの送信を依頼すると、当該メールの依頼履歴データを作成し、所定のフ

ァイルに蓄積する（Ｓ１０８）。ここで作成された依頼履歴データは、第一の実施の形態と同じ図４に示す依頼履歴データと図７に示す動作履歴データとを含む。

【０１４８】

依頼履歴データの蓄積が完了すると、メールクライアント３のＣＰＵは比較必要条件チェックプログラム１２ａを実行する。比較必要条件チェックプログラム１２ａは、比較必要条件設定プログラム１１により設定された送信条件データと、蓄積した依頼履歴データとの比較処理を行う（Ｓ１０９）。尚、比較内容についてはメールサーバ５における比較必要条件チェックプログラム１２ｂの比較内容と同じであるため説明を省略する。

【０１４９】

ステップ１０９で比較必要条件チェックプログラム１２ａが、送信履歴データが送信条件データを満たしていなと判断した場合、ステップ１０２に戻り同様の処理を繰り返す。

【０１５０】

一方、ステップ１０９で比較必要条件チェックプログラム１２ａが、依頼履歴データが送信条件データを満たしていると判断した場合、比較必要条件チェックプログラム１２ａはメールサーバ５に送信履歴データの送信要求処理を行う（Ｓ１１０）。

【０１５１】

メールクライアント３のＣＰＵは、メールサーバ５から送信された送信履歴データを受信したことを受けて、履歴チェックプログラム１３を実行する（Ｓ１１１）。

【０１５２】

履歴チェックプログラム１３は、図４に示すメールクライアント３に蓄積された依頼履歴データと図５に示すメールサーバ５に蓄積された送信履歴データとを比較する。尚、比較内容については第一の実施の形態中で説明した「比較例」と同様であるため説明を省略する。

【０１５３】

ステップ１１１で、履歴チェックプログラム１３が双方のデータに相違は無いと判断した場合、ステップ１０２に戻り同様の処理を繰り返す。つまり、メールクライアント３から送信したメールと、メールサーバ５が送信を依頼されたメールとは同一のメールである場合、メールクライアント３がウイルスに感染している可能性は低いとみなされる。

【０１５４】

一方、履歴チェックプログラム１３が双方のデータに差異があると判断した場合、ウイルスに感染している可能性が高いと考えられる。そこで、履歴チェックプログラム１３は、ウイルスに感染している可能性が高いという旨をメールクライアント３のディスプレイに表示する等して利用者に通知する（Ｓ１１２）。

【０１５５】

以上の手順を経ることにより、メール送信を実行するウイルスが存在する可能性を報知することができる。

【０１５６】

上述したように本実施形態の異常検出システム・方法は、メールクライアント側で履歴チェックプログラムを実行する構成である。そのため、メールサーバがウイルスに感染してしまった場合においても、メールクライアント側で異常検出を支援することができる。これによって、ウイルスの感染を最小限に抑えることができる。

【０１５７】

第一実施形態又は第二実施形態に示した構成によれば、サーバとクライアントとの間で整合しない動作一般に起因するコンピュータの動作不良を検出できる。このような動作不良は、コンピュータウイルスを原因とするものに限定されない。

【０１５８】

（変形例１）

本実施形態の変形例１として、第一の実施の形態及び第二の実施の形態で説明した履歴比較プログラムの実行をメールクライアント及びメールサーバの双方で行う構成を挙げることができる。この変形例１は、メールクライアントのＨＤ及

びメールサーバのＨＤに履歴比較プログラムをインストールすることにより実現可能となる。

【０１５９】

（変形例２）

また、本実施形態の変形例２として、上記実施形態の変形例と同様、メールクライアント３の依頼履歴データ又は動作履歴データと送信条件とを比較することによってウイルスの存在を検知しても良い。例えば、図６に示す送信条件データ例中のＬ４に記載の「一定時間内にクライアントが許可する送信可能なメールの数」を５０通と設定する。尚、ここでの一定時間とは、メールソフトが起動している時間とする。この送信条件と、図７に示す動作履歴データ中の「起動時間中の送信処理の数」とを比較する。比較により、起動時間中の送信処理の数が５０通を超えている場合は、ウイルスがメールソフトを利用してメールを送信しているか、メールソフトに何らかの異常が発生した可能性が高いとみることができる。

【０１６０】

＜その他の実施の形態＞

また、本発明のその他の実施形態として、メールクライアント及びメールサーバ以外の装置（以下チェック装置と称す）が、本発明のチェックプログラムを実行する形態を例示できる。このような形態の場合、メールクライアントとメールサーバは、各々が蓄積した履歴データ（依頼履歴データ，動作履歴データ，送信履歴データ）をチェック装置に送信する。チェック装置は、チェックプログラムを実行し、メールクライアントの履歴データとメールサーバの履歴データとを比較する。

【０１６１】

＜その他＞

さらに、本実施形態は以下の発明を開示する。また、以下の発明（以下付記と称す）の何れかに含まれる構成要素を他の付記の構成要素と組み合わせても良い。

（付記１）

電子メールの送信を依頼するコンピュータにネットワークを介して電子メール送信サービスを提供するサーバが、前記コンピュータの動作異常を検出する方法であり、

前記コンピュータから電子メールの送信依頼を受け付けるステップと、

前記送信依頼を受けた電子メールを送信するステップと、

送信した電子メールに係る送信履歴情報を蓄積するステップと、

前記コンピュータに蓄積されている電子メールの送信依頼履歴に係る依頼履歴情報を参照するステップと、

前記送信履歴情報と前記依頼履歴情報とを比較するステップと、

前記比較結果に基づいて前記コンピュータの動作異常を検出するステップと、

を含むサーバにおける異常検出方法。

（付記２）

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認するステップと、

前記ステップによる確認結果が所定の基準を満たした場合に、前記依頼履歴情報を参照し、当該依頼履歴情報と前記送信履歴情報とを比較するステップと、

を含む付記１に記載のサーバにおける異常検出方法。

（付記３）

電子メールの送信を依頼するコンピュータにネットワークを介して電子メール送信サービスを提供するサーバが、前記コンピュータの動作異常を検出する方法であり、

前記コンピュータから電子メールの送信依頼を受け付けるステップと、

前記送信依頼を受けた電子メールを送信するステップと、

送信した電子メールに係る送信履歴情報を蓄積するステップと、

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にし

たがって確認するステップと、

前記確認結果に基づいて前記コンピュータの動作異常を検出するステップと、

を含むサーバにおける異常検出方法。

（付記４）

コンピュータの動作異常が検出されたことを当該コンピュータに報知するステップを含む付記１又は３に記載のサーバにおける異常検出方法。

（付記５）

前記コンピュータ上でメール送信を依頼するメールソフトの動作履歴情報を参照するステップと、

当該動作履歴情報と前記送信履歴情報とを比較するステップと、

前記送信履歴情報の内容が前記動作履歴情報の内容と所定の関係にあるときに前記コンピュータの動作異常を検出するステップと、

を含む付記１～４のいずれかに記載のサーバにおける異常検出方法。

（付記６）

前記サーバは、前記電子メールを送信先へ中継する中継装置である付記１～５の何れかに記載のサーバにおける異常検出方法。

（付記７）

電子メールの送信を依頼するコンピュータにネットワークを介して電子メール送信サービスを提供するサーバが、前記コンピュータの動作異常を検出する方法であり、

前記コンピュータから電子メールの送信依頼を受け付けるステップと、

前記送信依頼を受けた電子メールを送信するステップと、

送信した電子メールに係る送信履歴情報を蓄積するステップと、

前記送信履歴情報を前記コンピュータに参照させるステップと、

前記送信履歴情報に基づいて前記コンピュータに、前記コンピュータの動作異常を確認させるステップと、

を含むサーバにおける異常検出方法。

（付記８）

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステッ

プと、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認するステップと、

前記ステップによる確認結果が所定の基準を満たした場合に、前記送信履歴情報を前記コンピュータに参照させるステップと、

を含む付記７に記載のサーバにおける異常検出方法。

（付記９）

電子メールの送信を依頼するコンピュータと該コンピュータからの依頼に応じて電子メールを送信するサーバとからなる電子メールシステムで実行される前記コンピュータの動作異常を検出する方法であり、

前記コンピュータによる電子メールの送信依頼履歴に係る依頼履歴情報を参照するステップと、

前記サーバによる電子メールの送信履歴情報を参照するステップと、

前記依頼履歴情報と前記送信履歴情報とを比較するステップと、

前記比較結果に基づいて前記コンピュータの動作異常を検出するステップと、からなる異常検出方法。

（付記１０）

電子メール送信サービスを提供するサーバにネットワークを介して電子メールの送信を依頼するコンピュータが、当該コンピュータの動作異常を検出する方法であり、

前記サーバに電子メールの送信を依頼するステップと、

送信を依頼した電子メールに係る依頼履歴情報を蓄積するステップと、

前記サーバに蓄積されている電子メールの送信履歴に係る送信履歴情報を参照するステップと、

前記依頼履歴情報と前記送信履歴情報とを比較するステップと、

前記比較結果に基づいて動作異常を検出するステップと、

を含むコンピュータにおける異常検出方法。

（付記１１）

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステッ

プと、

最新に送信された電子メールを含む前記依頼履歴情報を前記送信確認条件にしたがって確認するステップと、

前記ステップによる確認結果が所定の基準を満たした場合に、前記送信履歴情報を参照し、当該送信履歴情報と前記依頼履歴情報とを比較するステップと、

を含む付記１０に記載のコンピュータにおける異常検出方法。

（付記１２）

前記コンピュータ上でメール送信を依頼するメールソフトの動作履歴情報を参照するステップと、

当該動作履歴情報と前記送信履歴情報とを比較するステップと、

前記送信履歴情報の内容が前記動作履歴情報の内容と所定の関係にあるときに前記コンピュータの動作異常を検出するステップと、

を含む付記１０又は１１に記載のコンピュータにおける異常検出方法。

（付記１３）

電子メール送信サービスを提供するサーバにネットワークを介して電子メールの送信を依頼するコンピュータが、当該コンピュータの動作異常を検出する方法であり、

電子メールを送信するステップと、

送信した電子メールに係る履歴情報を蓄積するステップと、

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記履歴情報を前記送信確認条件にしたがって確認するステップと、

前記確認結果に基づいて動作異常を検出するステップと、

を含むコンピュータにおける異常検出方法。

（付記１４）

コンピュータの動作異常が検出されたことを当該コンピュータに報知するステップを含む付記１０～１３の何れかに記載のコンピュータにおける異常検出方法。

（付記１５）

電子メール送信サービスを提供するサーバにネットワークを介して電子メールの送信を依頼するコンピュータが、当該コンピュータの動作異常を検出する方法であり、

前記サーバに電子メールの送信を依頼するステップと、

送信を依頼した電子メールに係る依頼履歴情報を蓄積するステップと、

前記依頼履歴情報を前記サーバに参照させるステップと、

を備え、

前記依頼履歴情報に基づいて前記サーバに、前記コンピュータの動作異常を確認させるコンピュータにおける異常検出方法。

（付記１６）

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認するステップと、

前記ステップによる確認結果が所定の基準を満たした場合に、前記依頼履歴情報を前記コンピュータに参照させるステップと、

をさらに含む付記１３～１５の何れかに記載のコンピュータにおける異常検出方法。

（付記１７）

電子メールの送信を依頼するコンピュータにネットワークを介して電子メール送信サービスを提供するサーバが前記コンピュータの動作異常を検出するためのプログラムであり、

前記サーバに、

前記コンピュータからの電子メールの送信依頼に基づき送信された電子メールに係る送信履歴情報を参照するステップと、

前記コンピュータによる電子メールの送信依頼履歴に係る依頼履歴情報を参照するステップと、

前記送信履歴情報と前記依頼履歴情報とを比較するステップと、

前記比較結果に基づいて前記コンピュータの動作異常を検出するステップと、
を実行させる異常検出プログラム。

（付記１８）

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認するステップと、

前記ステップによる確認結果が所定の基準を満たした場合に、前記依頼履歴情報を参照し、当該依頼履歴情報と前記送信履歴情報とを比較するステップと、
を含む付記１７に記載の異常検出プログラム。

（付記１９）

電子メールの送信を依頼するコンピュータにネットワークを介して電子メール送信サービスを提供するサーバが前記コンピュータの動作異常を検出するためのプログラムであり、

前記サーバに、

前記コンピュータからの電子メールの送信依頼に基づき送信された電子メールに係る送信履歴情報を参照するステップと、

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認するステップと、

前記確認結果に基づいて前記コンピュータの動作異常を検出するステップと、
を実行させる異常検出プログラム。

（付記２０）

前記コンピュータ上でメール送信を依頼するメールソフトの動作履歴情報を参照するステップと、

当該動作履歴情報と前記送信履歴情報とを比較するステップと、

前記送信履歴情報の内容が前記動作履歴情報の内容と所定の関係にあるときに前記コンピュータの動作異常を検出するステップと、

を含む付記１７～１９の何れかに記載の異常検出プログラム。

（付記２１）

前記サーバは、前記電子メールを送信先へ中継する中継装置である付記１７～２０の何れか記載の異常検出プログラム。

（付記２２）

コンピュータの動作異常が検出されたことを当該コンピュータに報知するステップを含む付記１７～２１の何れかに記載の異常検出プログラム。

（付記２３）

電子メールの送信を依頼するコンピュータにネットワークを介して電子メール送信サービスを提供するサーバが前記コンピュータの動作異常を検出するためのプログラムであり、

前記サーバに、

前記コンピュータからの電子メールの送信依頼に基づき送信され蓄積された電子メールに係る送信履歴情報を前記コンピュータに参照させるステップと、

前記送信履歴情報に基づいて前記コンピュータに、前記コンピュータの動作異常を確認させるステップと、

を実行させる異常検出プログラム。

（付記２４）

電子メールの送信を依頼するコンピュータと該コンピュータからの依頼に応じて電子メールを送信するサーバとからなる電子メールシステムで実行され、

前記コンピュータによる電子メールの送信依頼履歴に係る依頼履歴情報を参照するステップと、

前記サーバによる電子メールの送信履歴情報を参照するステップと、

前記依頼履歴情報と前記送信履歴情報とを比較するステップと、

前記比較結果に基づいて前記コンピュータの動作異常を検出するステップと、

を実行させる異常検出プログラム。

（付記２５）

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認するステップと、

前記確認手段による確認結果が所定の基準を満たした場合に、前記送信履歴情報を前記コンピュータに参照させるステップと、

を含む付記２３又は２４に記載の異常検出プログラム。

（付記２６）

電子メール送信サービスを提供するサーバにネットワークを介して電子メールの送信を依頼するコンピュータが、当該コンピュータの動作異常を検出するためのプログラムであり、

コンピュータに、

前記サーバに電子メールの送信を依頼した電子メールに係る依頼履歴情報を参照するステップと、

前記サーバに蓄積されている電子メールの送信履歴に係る送信履歴情報を参照するステップと、

前記依頼履歴情報と前記送信履歴情報とを比較するステップと、

前記比較結果に基づいて動作異常を検出するステップと、

を実行させる異常検出プログラム。

（付記２７）

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記依頼履歴情報を前記送信確認条件にしたがって確認するステップと、

前記ステップによる確認結果が所定の基準を満たした場合に、前記送信履歴情報を参照し、当該送信履歴情報と前記依頼履歴情報とを比較するステップと、

を含む付記２６に記載の異常検出プログラム。

（付記２８）

前記コンピュータ上でメール送信を依頼するメールソフトの動作履歴情報を参照するステップと、

当該動作履歴情報と前記送信履歴情報とを比較するステップと、

前記送信履歴情報の内容が前記動作履歴情報の内容と所定の関係にあるときに前記コンピュータの動作異常を検出するステップと、
を含む付記２６又は２７に記載の異常検出プログラム。
（付記２９）
電子メール送信サービスを提供するサーバにネットワークを介して電子メールの送信を依頼するコンピュータが、当該コンピュータの動作異常を検出するためのプログラムであり、
前記コンピュータに、
送信した電子メールに係る履歴情報を蓄積するステップと、
前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、
最新に送信された電子メールを含む前記履歴情報を前記送信確認条件にしたがって確認するステップと、
前記確認結果に基づいて動作異常を検出するステップと、
を実行させる異常検出プログラム。
（付記３０）
コンピュータの動作異常が検出されたことを当該コンピュータに報知するステップを含む付記２４～２９の何れかに記載の異常検出プログラム。
（付記３１）
電子メール送信サービスを提供するサーバにネットワークを介して電子メールの送信を依頼するコンピュータが、当該コンピュータの動作異常を検出するためのプログラムであり、
前記コンピュータに、
前記サーバに送信を依頼した電子メールに係る依頼履歴情報を蓄積するステップと、
前記依頼履歴情報を前記サーバに参照させるステップと、
前記依頼履歴情報に基づいて前記サーバに、前記コンピュータの動作異常を確認させるステップと、
を実行させる異常検出プログラム。

（付記３２）

前記コンピュータにおける電子メール送信時の送信確認条件を参照するステップと、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認するステップと、

前記ステップで確認結果が所定の基準を満たした場合に、前記依頼履歴情報を前記コンピュータに参照させるステップと、

を含む付記２９又は３０に記載の異常検出プログラム。

（付記３３）

電子メールの送信を依頼するコンピュータに電子メール送信サービスを提供するサーバであり、

前記コンピュータから電子メールの送信依頼を受け付ける受付手段と、

前記送信依頼を受けた電子メールを送信する送信手段と、

送信した電子メールに係る送信履歴情報を蓄積する蓄積手段と、

前記コンピュータに蓄積されている電子メールの送信依頼履歴に係る依頼履歴情報を前記コンピュータから参照する履歴参照手段と、

前記送信履歴情報と前記依頼履歴情報とを比較する比較手段と、

前記比較結果に基づいて前記コンピュータの動作異常を検出する検出手段と、

を備えるサーバ。

（付記３４）

前記コンピュータにおける電子メール送信時の送信確認条件を参照する条件参照手段と、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認する確認手段とをさらに備え、

前記確認手段による確認結果が所定の基準を満たした場合に、前記履歴参照手段は、前記依頼履歴情報を参照し、前記比較手段は前記送信履歴情報と前記依頼履歴情報とを比較する付記３３に記載のサーバ。

（付記３５）

電子メールの送信を依頼するコンピュータに電子メール送信サービスを提供す

るサーバであり、

前記コンピュータから電子メールの送信依頼を受け付ける受付手段と、

前記送信依頼を受けた電子メールを送信する送信手段と、

送信した電子メールに係る送信履歴情報を蓄積する蓄積手段と、

前記コンピュータにおける電子メール送信時の送信確認条件を参照する条件参照手段と、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認する確認手段と、

前記確認結果に基づいて前記コンピュータの動作異常を検出する検出手段と、を備えるサーバ。

（付記３６）

コンピュータの動作異常が検出されたことを当該コンピュータに報知する報知手段を有する付記３３～３５の何れかに記載のサーバ。

（付記３７）

前記依頼履歴情報は、前記コンピュータ上でメール送信を依頼するメールソフトの動作履歴情報を参照する手段をさらに備え、

前記比較手段は、前記送信履歴情報と前記メールソフトの動作履歴情報とを比較する手段を有し、

前記検出手段は、前記送信履歴情報の内容が前記動作履歴情報の内容と所定の関係にあるときに前記コンピュータの動作異常を検出する請求項３３～３６の何れかに記載のサーバ。

（付記３８）

前記サーバは、前記電子メールを送信先へ中継する中継装置である付記３３～３７の何れかに記載のサーバ。

（付記３９）

電子メールの送信を依頼するコンピュータに電子メール送信サービスを提供するサーバであり、

前記コンピュータから電子メールの送信依頼を受け付ける受付手段と、

前記送信依頼を受けた電子メールを送信する送信手段と、

送信した電子メールに係る送信履歴情報を蓄積する蓄積手段と、

前記送信履歴情報を前記コンピュータに参照させる参照指示手段と、

を備え、

前記送信履歴情報に基づいて前記コンピュータに、前記コンピュータの動作異常を確認させるサーバ。

（付記４０）

前記コンピュータにおける電子メール送信時の送信確認条件を参照する条件参照手段と、

最新に送信された電子メールを含む前記送信履歴情報を前記送信確認条件にしたがって確認する確認手段と、

をさらに備え、

前記参照指示手段は、前記確認手段による確認結果が所定の基準を満たした場合に、前記送信履歴情報を前記コンピュータに参照させる付記３９に記載のサーバ。

（付記４１）

電子メール送信サービスを提供するサーバに電子メールの送信を依頼するコンピュータであり、

前記サーバに電子メールの送信を依頼する依頼手段と、

送信を依頼した電子メールに係る依頼履歴情報を蓄積する蓄積手段と、

前記サーバに蓄積されている電子メールの送信履歴に係る送信履歴情報を前記サーバから参照するサーバ履歴参照手段と、

前記依頼履歴情報と前記送信履歴情報とを比較する比較手段と、

前記比較結果に基づいて動作異常を検出する検出手段と、

を備えるコンピュータ。

（付記４２）

電子メールの送信をサーバに依頼するコンピュータによる電子メールの送信依頼履歴に係る依頼履歴情報を参照する第一参照手段と、

前記電子メールの依頼に応じて電子メールを送信する前記サーバによる電子メールの送信履歴情報を参照する第二参照手段と、

前記依頼履歴情報と前記送信履歴情報とを比較する比較手段と、

前記比較結果に基づいて前記コンピュータの動作異常を検出する検出手段と、

を備えることを特徴とするコンピュータ。

（付記４３）

前記コンピュータにおける電子メール送信時の送信確認条件を参照する条件参照手段と、

最新に送信された電子メールを含む前記依頼履歴情報を前記送信確認条件にしたがって確認する確認手段と、

をさらに備え、

前記確認手段による確認結果が所定の基準を満たした場合に、前記サーバにおける前記履歴参照手段は、前記送信履歴情報を参照し、前記比較手段は前記送信履歴情報と前記依頼履歴情報とを比較する付記４１に記載のコンピュータ。

（付記４４）

前記コンピュータ上でメール送信するメールソフトの動作履歴情報を参照する動作履歴参照手段をさらに備え、

前記比較手段は、前記依頼履歴情報と前記動作履歴情報とを比較する比較手段を有し、

前記検出手段は、前記履歴情報の内容が前記動作履歴情報の内容と所定の関係にあるときに前記動作異常を検出する請求項４１～４３の何れかに記載のコンピュータ。

（付記４５）

電子メール送信サービスを提供するサーバに電子メールの送信を依頼するコンピュータであり、

電子メールを送信する手段と、

送信した電子メールに係る履歴情報を蓄積する手段と、

前記コンピュータにおける電子メール送信時の送信確認条件を参照する条件手段と、

最新に送信された電子メールを含む前記履歴情報を前記送信確認条件にしたがって確認する確認手段と、

前記確認結果に基づいて動作異常を検出する検出手段と、
を備えるコンピュータ。
（付記４６）
コンピュータの動作異常が検出されたことを当該コンピュータに報知する報知手段を有する付記４１～４５の何れかに記載のコンピュータ。
（付記４７）
電子メール送信サービスを提供するサーバに電子メールの送信を依頼するコンピュータであり、
前記サーバに電子メールの送信を依頼する手段と、
送信を依頼した電子メールに係る依頼履歴情報を蓄積する蓄積手段と、
前記依頼履歴情報を前記サーバに参照させる参照指示手段と、
を備え、
前記依頼履歴情報に基づいて前記サーバに、前記コンピュータの動作異常を確認させるコンピュータ。
（付記４８）
前記コンピュータにおける電子メール送信時の送信確認条件を参照する条件参照手段と、
最新に送信された電子メールを含む前記依頼履歴情報を前記送信確認条件にしたがって確認する依頼履歴確認手段と、
をさらに備え、
前記参照指示手段は、前記依頼履歴確認手段による確認結果が所定の基準を満たした場合に、前記依頼履歴情報を前記サーバに参照させる付記４７に記載のコンピュータ。

【０１６２】

【発明の効果】

以上のことにより、本発明によれば、ウイルスやその他に起因するコンピュータの動作異常を検出する異常検出方法、異常検出プログラム、サーバ、コンピュータを提供することが可能となる。

【０１６３】

また、本発明によれば、パターンファイルの更新を要することなく、未知のコンピュータウイルスの手がかりを発見する異常検出方法、異常検出プログラム、サーバ、コンピュータを提供することができる。

【図面の簡単な説明】

【図１】

第一の実施の形態に係るメール送信システムの概念図である。

【図２】

ウイルスが独自のメールエンジンを利用してメールを送信するときの概念図である。

【図３】

第一の実施の形態に係るシステム構成図である。

【図４】

第一の実施の形態及び第二の実施の形態に係るメールクライアントにおける依頼履歴データの一覧である。

【図５】

第一の実施の形態及び第二の実施の形態に係るメールサーバにおける送信履歴データの一覧である。

【図６】

第一の実施の形態及び第二の実施の形態に係る比較必要条件設定プログラムによる設定内容の一覧である。

【図７】

第一の実施の形態及び第二の実施の形態にかかるメールクライアントにおける動作履歴データの一覧である。

【図８】

第一の実施の形態に係る異常検出手順を示すフローチャートである。

【図９】

第二の実施の形態に係るシステム構成図である。

【図１０】

第二の実施の形態に係る異常検出手順を示すフローチャートである。

【符号の説明】

１　メール送信システム

２　メール

３　メールクライアント

４　メールソフト

５　メールサーバ

６　ユーザインターフェース

７　メール送信エンジン

７ｂ　メール送信エンジン

８ａ　送信条件データファイル

８ｂ　送信条件データファイル

９　動作履歴データファイル

１０ａ　依頼履歴データファイル

１０ｂ　送信履歴データファイル

１１　比較必要条件設定プログラム

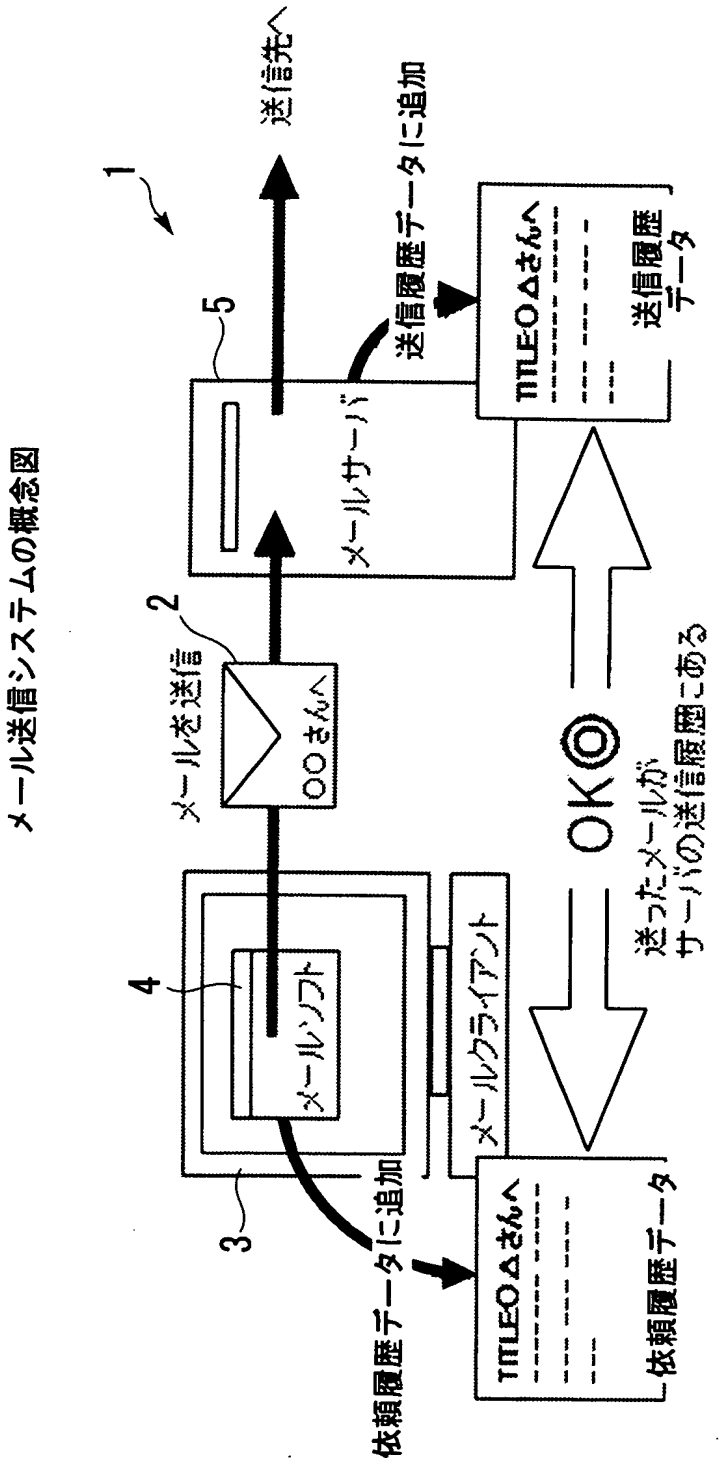
１２ａ　比較必要条件チェックプログラム

１２ｂ　比較必要条件チェックプログラム

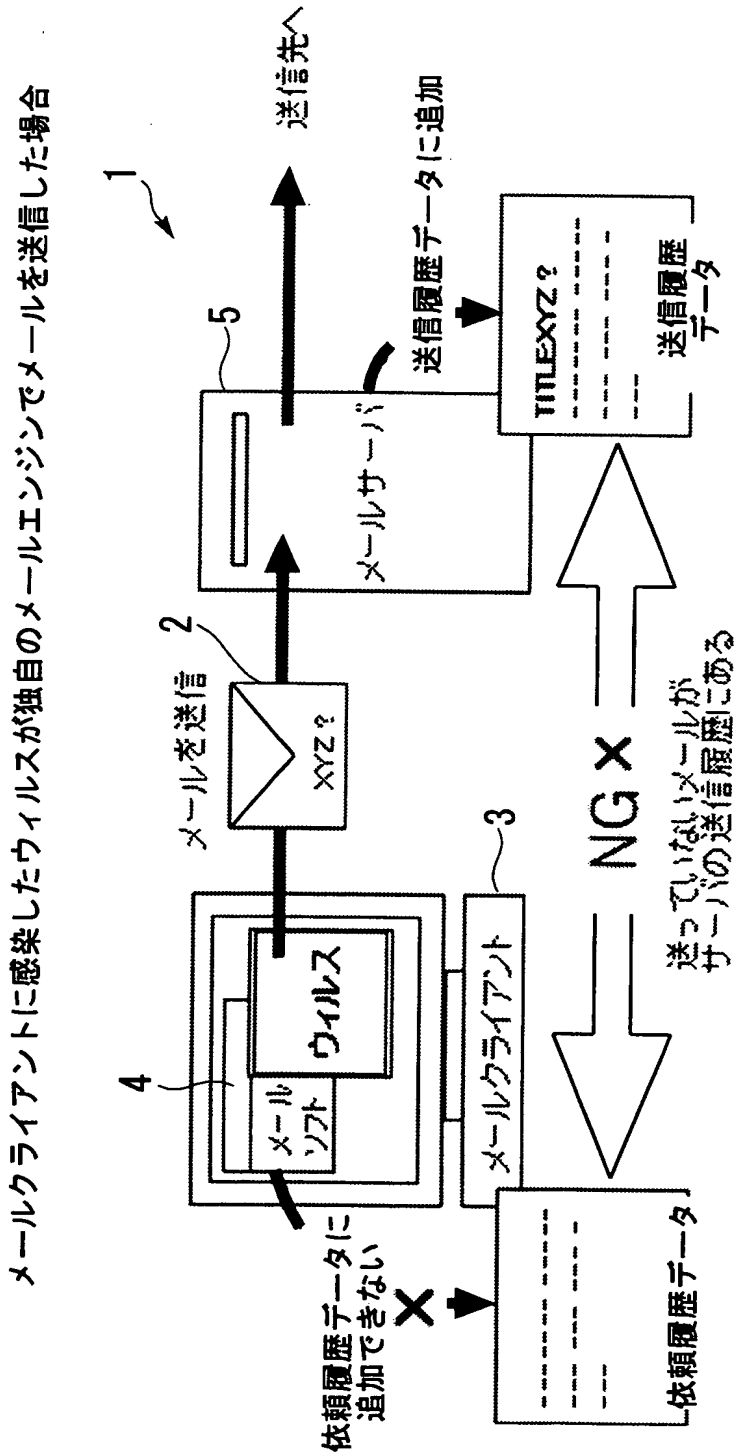
１３　履歴チェックプログラム

【書類名】　図面

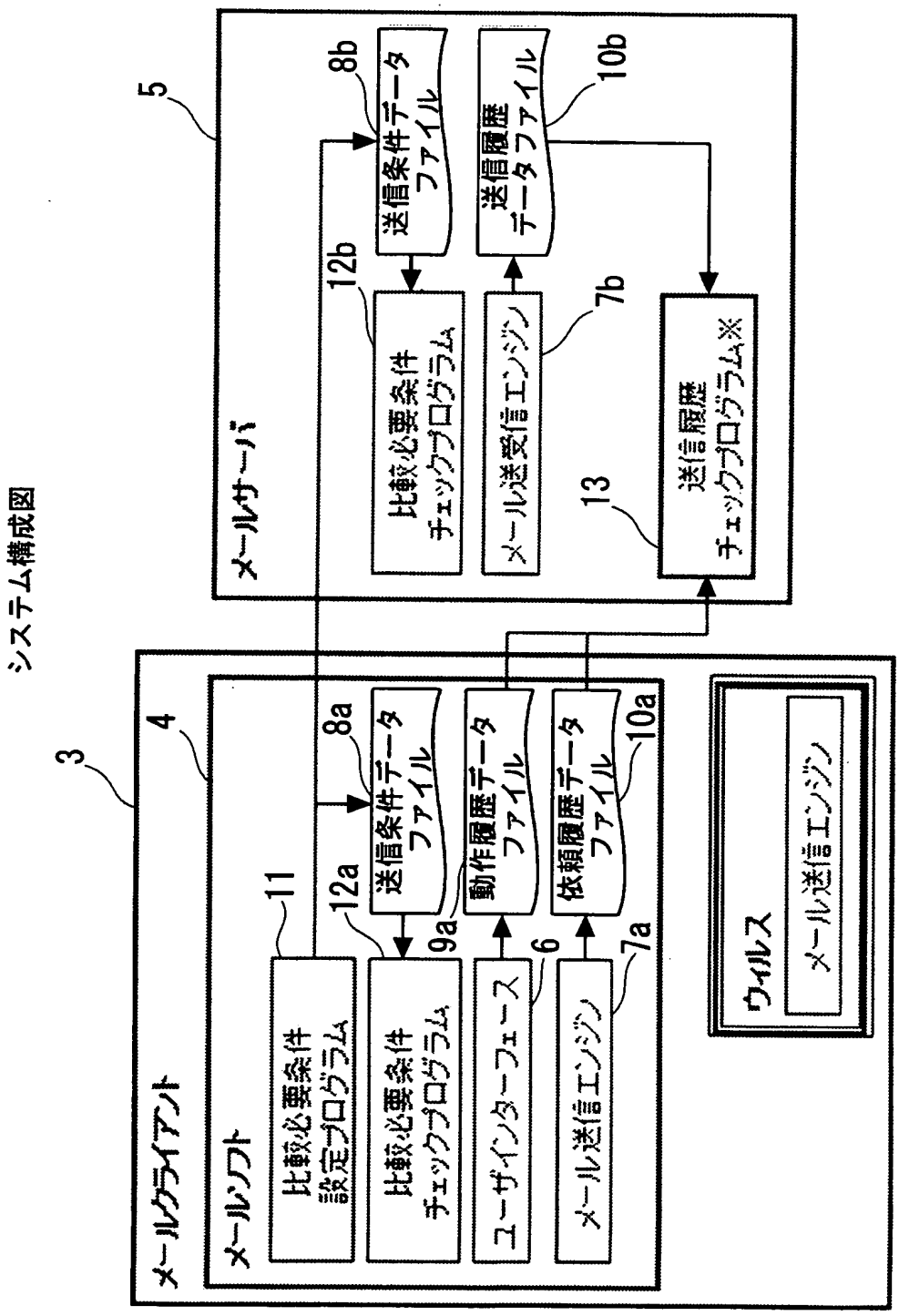
【図１】


メール送信システムの概念図
1
2
メールを送信
○○さんへ
3
4
メールソフト
メールクライアント
5
メールサーバ
送信先へ
送信履歴データに追加
TTLEO△さんへ
送信履歴データ
OK◎
送ったメールがサーバの送信履歴にある
依頼履歴データに追加
TTLEO△さんへ
依頼履歴データ

【図２】


メールクライアントに感染したウィルスが独自のメールエンジンでメールを送信した場合
1
送信先へ
送信履歴データに追加
5
メールサーバ
TITLEXYZ？
送信履歴
データ
2
メールを送信
XYZ？
3
メールクライアント
NG
送ったがいないメールが
サーバの送信履歴にある
4
ウィルス
メール
ソフト
依頼履歴データに
追加できない
依頼履歴データ

【図３】


システム構成図
メールクライアント
3
メールソフト
4
比較必要条件
設定プログラム
11
比較必要条件
チェックプログラム
12a
ユーザインターフェース
6
メール送信エンジン
7a
送信条件データ
ファイル
8a
動作履歴データ
ファイル
9a
依頼履歴データ
ファイル
10a
ウィルス
メール送信エンジン
メールサーバ
5
送信条件データ
ファイル
8b
送信履歴
データファイル
10b
比較必要条件
チェックプログラム
12b
メール送受信エンジン
7b
送信履歴
チェックプログラム※
13

【図４】

●メールクライアント

送信履歴データの例

	記述内容	記述例
	履歴全体	
	メールの総数	80
	もっとも古いメールの日時	2002/10/22 11:00:01
	最新のメールの日時	2002/11/21 10:00:32
	各メール(各メールに対して以下(1~8)の情報を用意する)	
1	題名	○○さんへ
2	送信元	watashi@ccc.ddd.com
3	送信先(複数可)	marumaru@aaa.bbb.ne.jp
4	添付ファイルの有無	有
5	添付ファイル名(複数可)	photo.gif
6	本文※1	こんにちは、お元気ですか？先日はありが…
7	送信時間	2002/11/05 20:05:58
8	ヘッダ情報(複数可)	Content-Type:text/plain;…

【図５】

●メールサーバ

送信依頼履歴データの例

記述内容	記述例
履歴全体	
メールの総数	80
もっとも古いメールの日時	2002/10/22 11:00:01
最新のメールの日時	2002/11/21 10:00:32
各メール(各メールに対して以下(1～10)の情報を用意する)	
1 題名	○○さんへ
2 送信元	watashi@ccc.ddd.com
3 送信先(複数可)	marumaru@aaa.bbb.ne.jp
4 添付ファイルの有無	有
5 添付ファイル名(複数可)	photo.gif
6 本文※1	こんにちは、お元気ですか？ 先日はありが…
7 受信時間	2002/11/05 20:06:10
8 送信時間	2002/11/05 20:06:50
9 ヘッダ情報(複数可)	Content-Type:text/plain;X-Mailer:…
10 受信経路(IP アドレスなど、サーバ側で分かる送信経路やクライアントを特定できる情報)	(クライアント、サーバの送信方法等によって保存できる情報が異なる)

※1 長文の場合、送信履歴データと別のデータとして管理してもよい

【図６】

送信条件データ例

	条件の内容	条件値
L1	前回履歴を比較した日時	2002/10/22 11:00:22
L2	前回の比較日時からどれだけ経過したら比較するか	2週間
L3	最新ウイルス情報を受け取ってから比較をしたか	比較済(または、未比較)
L4	一定時間内のメール送信数：クライアントが許可している数	50
L5	一定時間内のメール送信数：今までの最大送信数	23
L6	同じ内容のメール送信数：クライアントが許可している数	10
L7	同じ内容のメール送信数：今までの最大送信数	7

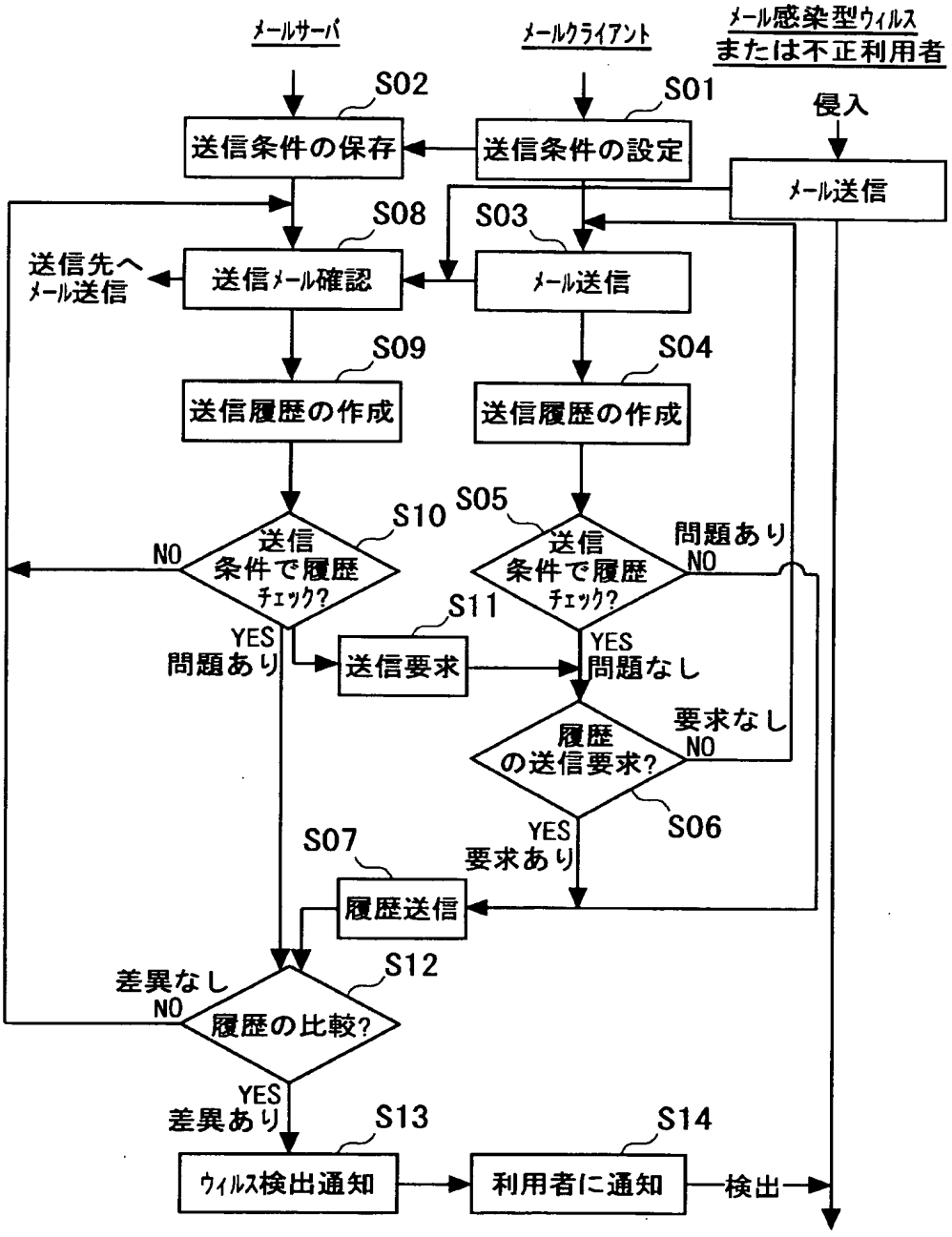
【図７】

動作履歴データの例

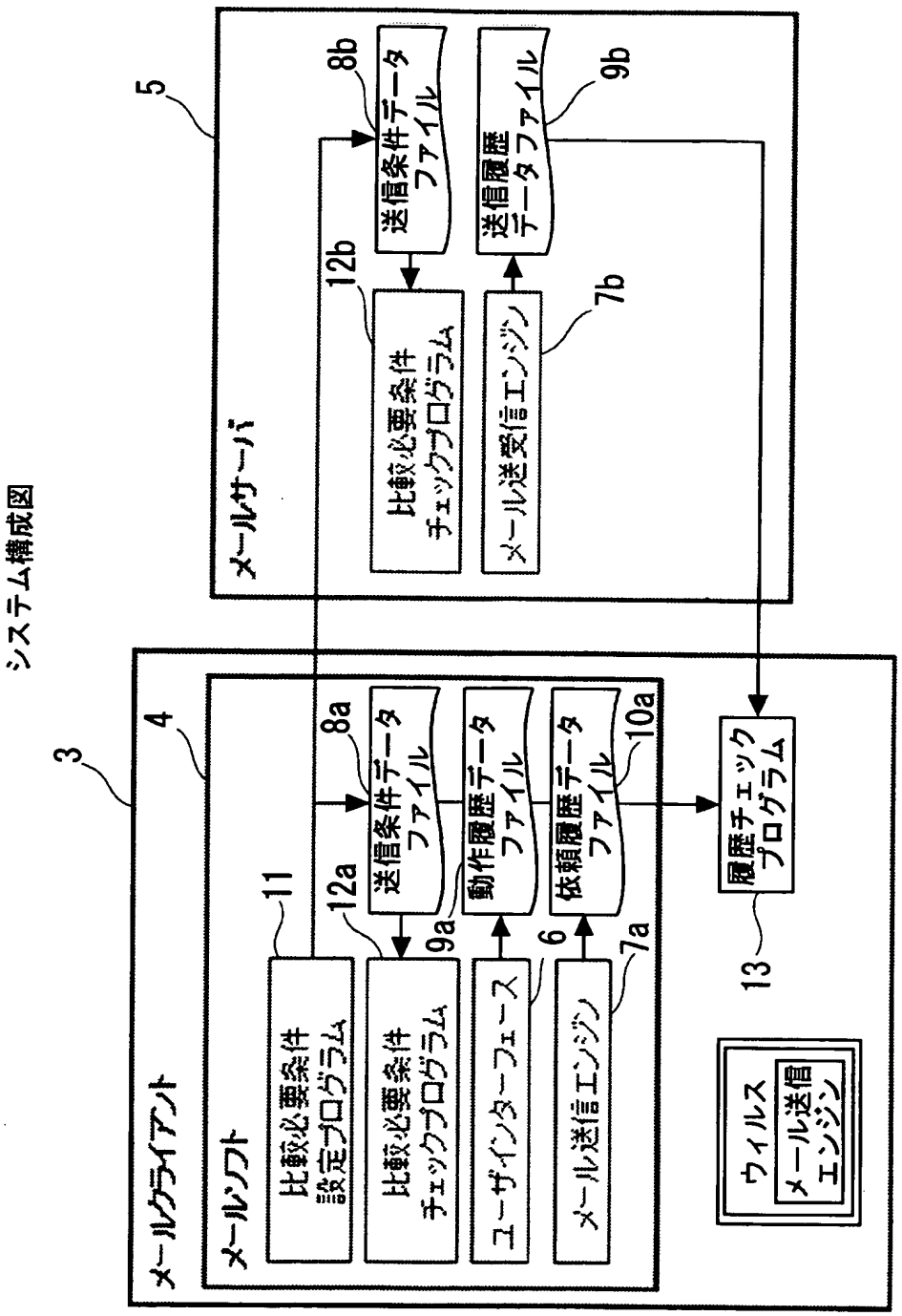
記述内容		記述例
全体		
動作記録を取得したメールの総数		78
もっとも古い動作記録を取得したメールの日時		2002/10/22 11:00:01
最新の動作記録を取得したメールの日時		2002/11/20 15:32:32
ソフト全般に関する履歴(以下(1～3)の情報を一回分の基本動作として、起動回数分記録する)		
1	起動時間	2002/11/20 14:52:01
2	終了時間	2002/11/20 16:03:46
3	起動時間中の送信処理の数	3
送信先/送信元に関する履歴(アドレス帳のアドレスすべてに対して、以下(1～3)の情報を記録する)		
1	アドレス名	marumaru@aaa.bbb.ne.jp
2	今までの送信回数	5
3	前回、送信した日時	2002/09/15 13:30:02
メール送信に関する履歴(以下(1～15)の情報を一回分の送信動作として、送信回数分記録する)		
1	題名	○○さんへ
2	題名の入力方法	キーボード入力(または、"Re:"+受信メールの題名等)
3	送信元	watashi@ccc.ddd.com
4	送信先(複数可)	marumaru@aaa.bbb.ne.jp
5	送信先の選択方法	キーボード入力(または、アドレス帳参照等)
6	メールの作成方法	新規(または、返信、転送等)
7	添付ファイルの有無	有
8	添付ファイル名(複数可)	C:¥mail¥sendmail¥data¥photo.gif
9	添付ファイルの選択方法	キーボード入力(または、ファイル参照等)
10	本文※1	こんにちは、お元気ですか？先日はありが・・・
11	本文入力の有無	キーボード入力(または、転送、コピーのみ等)
12	送信時間	2002/11/05 20:05:58
13	送信決定処理の有無	有
14	送信決定処理を行った画面/部品名	メニュー(または、ボタン等)
15	送信経過ダイアログの表示の有無	有

【図８】

メールサーバ側で履歴比較を行うフローチャート

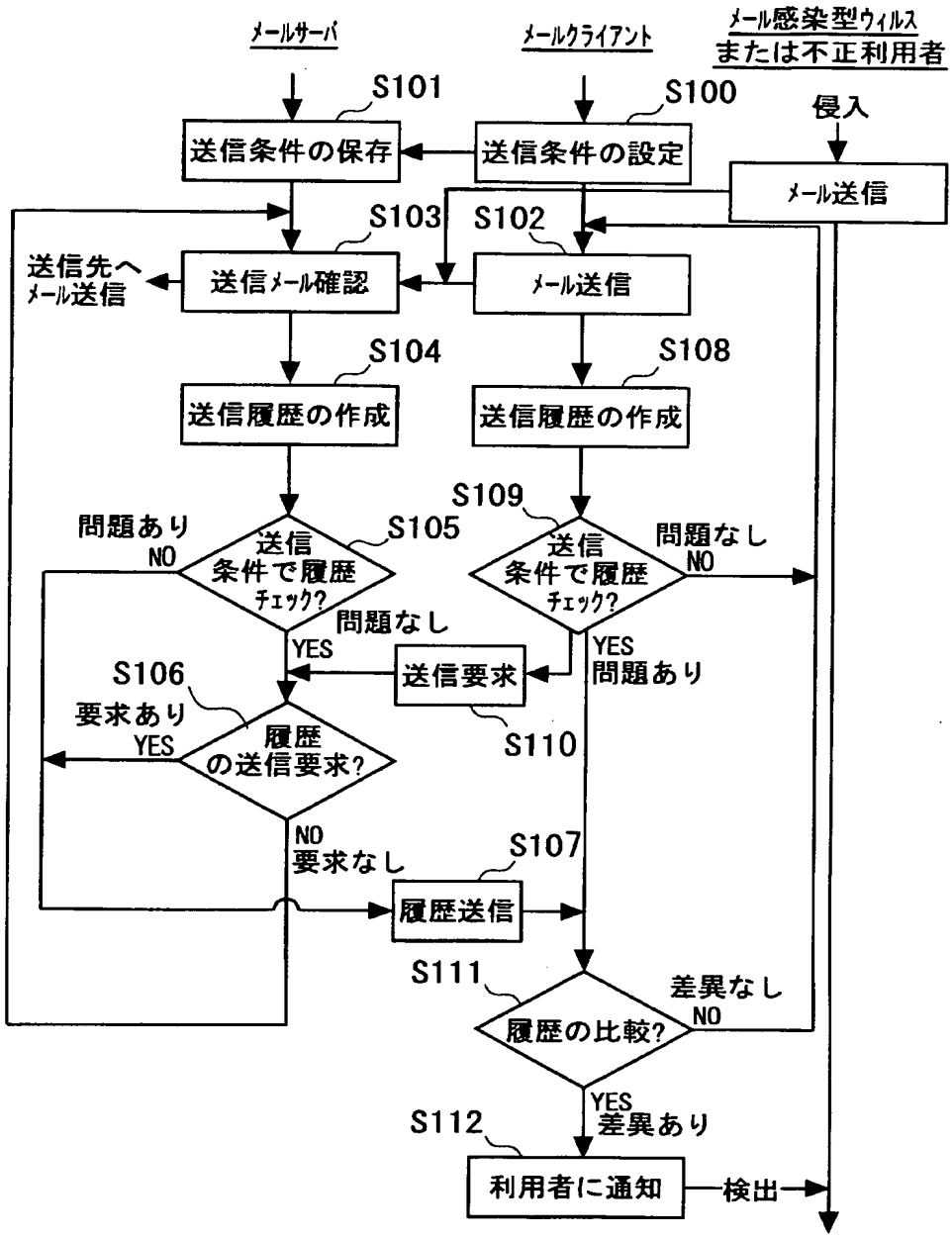


【図９】


システム構成図
メールクライアント
3
メールソフト
4
比較必要条件
設定プログラム
11
比較必要条件
チェックプログラム
12a
送信条件データ
ファイル
8a
動作履歴データ
ファイル
9a
ユーザインターフェース
6
依頼履歴データ
ファイル
10a
メール送信エンジン
7a
履歴チェック
プログラム
13
ウィルス
メール送信
エンジン
メールサーバ
5
比較必要条件
チェックプログラム
12b
送信条件データ
ファイル
8b
メール送受信エンジン
7b
送信履歴
データファイル
9b

【図１０】

メールクライアント側で履歴比較を行うフローチャート



【書類名】　要約書

【要約】

【課題】　本発明は、ウイルスやその他に起因するコンピュータの動作異常を検出する異常検出方法、異常検出プログラム、サーバ、コンピュータを提供することを課題とする。また、本発明によれば、パターンファイルの更新を要することなく、未知のコンピュータウイルスの手がかりを発見する異常検出方法、異常検出プログラム、サーバ、コンピュータを提供することを課題とする。

【解決手段】　本実施形態におけるメールサーバ５は、メールクライアント３に記録された依頼履歴データと、メールサーバ５に記録された送信履歴データとを比較する履歴比較チェックプログラム１３を備えている。

【選択図】　図３

特願２００３－０４９２５５

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社